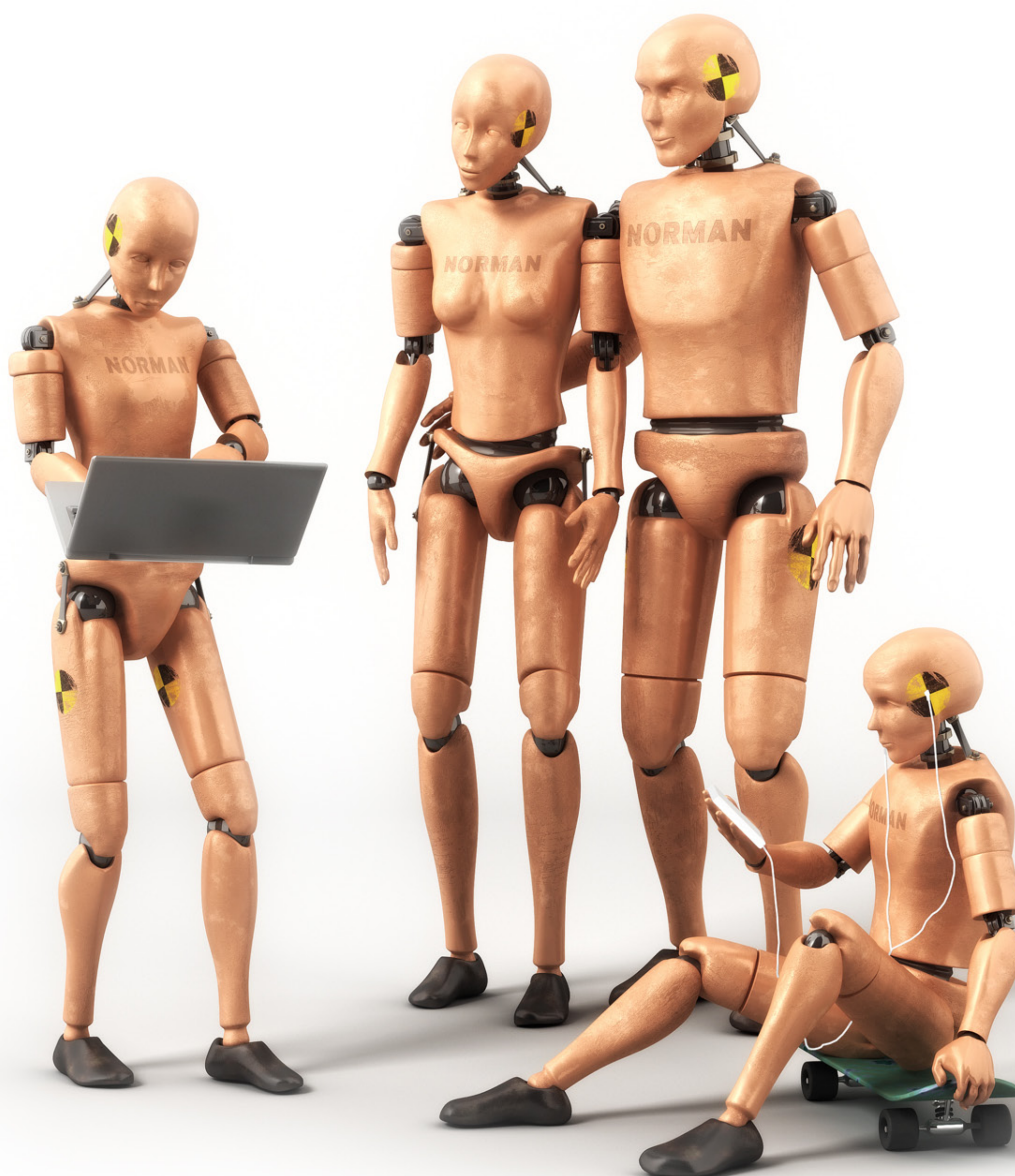
NORMAN®

SecuritySuite

使用手冊

版本 8.00





- Antivirus
- Antispam
- Intrusion Guard
- Personal Firewall
- Parental Control
- Privacy Tools

NORMAN®

有限瑕疵責任擔保

Norman 保證隨附之 CD-ROM 或 DVD 與文件絕無產品瑕疵。若您於購買之 30 天內通報瑕疵，Norman 將免費為您更換瑕疵 CD-ROM 或 DVD 和 / 或文件。任何申訴均須隨附購買證明。

本擔保僅限於更換產品。對於因使用本軟體或文件或其中之錯誤或缺陷所引起之任何形式損失或損壞，包括但不限於盈收損失，Norman 概不負責。

對於 CD-ROM、DVD、文件或此授權合約中之瑕疵或缺點，本擔保無論明示或默示，均優先於任何其他擔保，包括但不限於適售性及特定目的之適用性默示擔保。

尤其是未遵守本授權合約對於任何特殊使用或目的之限制，Norman 對於獲利損失或其他商業損壞，包括但不限於偶發或衍生性損害，概不負責。

此擔保會在購買後 30 天過期。

本文件資訊與軟體功能如有變更，恕不另行通知。請依照本授權合約條款使用本軟體。購買者可複製一份本軟體以供備份之用。未經 Norman 明確書面許可，本文件之任何部分均不得因任何非購買者個人使用之目的，以任何形式或使用任何電子或機械方法重製或傳輸，包括影印、錄音或存放於資訊儲存裝置和擷取系統中。

Norman 標誌為 Norman ASA 的註冊商標。

本文件中所提及之產品名稱為其各自擁有者之商標或註冊商標。本文件提及產品名稱僅供識別之用。

修訂於 2010 年 3 月。

簡介

系統需求

本版本支援根據以下規格，在 Windows XP、Windows Vista 與 Windows 7 電腦上安裝 Norman Security Suite v8.00：

Windows	XP	Vista	7
Antivirus	✓	✓	✓
Intrusion Guard	僅限 32 位元	✓	✓
Personal Firewall		✓	✓
Parental Control		✓	✓
Antispam [1]		✓	✓
Privacy Tools		✓	✓
Service Pack 或更高版本	2	1	
CPU (Pentium 系列) 建議	1.8 GHz		
RAM 建議	2 GB		
Internet Explorer 或更高版本	7 (8)		
可用磁碟空間 建議	500 MB		
螢幕解析度 建議	1024x768		

[1] Antispam 僅適用於 Windows Outlook、Outlook Express 與 Vista Mail。

關於本版本

本版本提供數種語言。新語言將不定期加入。如需您所使用語言之 Security Suite 相關資訊，請與您的 Norman 經銷商聯絡。如需詳細資訊，請瀏覽 Norman 網站，如需語言版本詳細資訊，請與您的當地經銷商聯絡。

關於本手冊

本手冊概述 Norman Security Suite 中的產品、功能與重要功用。如需所有可用選項之詳細說明，請參閱在線說明。



注釋：特殊或重要註釋的左邊界標記有驚嘆號。

訓練與技術支援

如需訓練或技術支援，請與當地經銷商或 Norman ASA 聯絡。Norman 提供 Security Suite 與一般安全問題之技術支援與諮詢服務。技術支援也包含防毒程式安裝之品質保證，包括專為 Security Suite 量身打造之協助，以符合您的真正需求。請注意，可用的服務數將因不同國家而改變。

本文件最後一頁顯示有關 Norman 辦公室的聯絡資訊。

何謂 Norman Security Suite ?

Norman Security Suite (NSS) 是軟體安全套裝軟體，由六個不同的安全應用程式所組成，分別是：

Antivirus & Antispyware	阻止病毒入侵您的電腦
Personal Firewall	阻止駭客使用您的電腦來傳輸不當流量
Antispam	阻止不需要的及大量的電子郵件
Parental Control	阻止年輕人造訪內容不宜的網站
Privacy Tools	協助您安全地刪除檔案及您的個人資料。
Intrusion Guard	阻止惡意程式入侵及感染您的電腦

* 后两个应用程序（Privacy Tools 和 Intrusion Guard）仅包含在 Security Suite PRO 版本中。

Norman Security Suite 在安裝後即可隨時使用。預設的配置設定即提供您所需的保護方法，因此您不必透過配置選項執行，即可讓程式運作。但是知道軟體的運作方式以及熟悉其基本功能，是很有幫助的。本手冊鎖定某些實用的功能，並提供一些如何充分利用本程式的建議。



注釋：您必須先執行精靈，才能開始使用 Personal Firewall。如需詳細資訊，請參閱第 12 頁的「安裝精靈」。

Antivirus & Antispyware

此防毒程式可監控您的個人電腦是否有惡意軟體。惡意軟體是病毒、蠕蟲、特洛伊病毒和其他各種有害程式碼。間諜軟體不像傳統的病毒一樣具有毀滅性，但無意洩露個人資訊的後果是很危險的。Norman 獨一無二的 Sandbox 可主動保護系統，甚至可找出未知的病毒。

如需 Norman 的 Sandbox 詳細資訊，請參閱第 63 頁。

病毒會自動從硬碟、抽取式媒體、電子郵件附件等中移除。Antivirus & Antispyware 應用程式會在存取檔案時檢查檔案，並自動移除可能的病毒。Security Suite 有兩個主要掃描器 – 自動掃描器和手動掃描器 – 以及不同的掃描方式。

我們鼓勵使用者手動掃描電腦，所以您可以即時從系統托盤功能表中開始掃描整台電腦。您也可以在瀏覽檔案時從右鍵功能表開始掃描，或者選擇 Norman 的螢幕保護程式，它也會在啟動時開始掃描病毒。當您繼續作業時，掃描便會中止，下一次螢幕保護程式啟動時，會從它離開的地方繼續掃描。如需定期手動掃描，您可以使用工作編輯器和排程器來定義電腦掃描的範圍和時間。

本產品出貨時已預先選擇了部分設定，這些設定是我們認為能夠充分保護您免遭病毒攻擊的設定。此外，模組也可以配置，讓您能夠設定應用程式以符合您真正的需求。

Personal Firewall

每次您連線到 Internet、讀取電子郵件或上網時，便與全世界的其他電腦建立連線 – 它們也與您的電腦連線。這就是麻煩的地方。駭客只要破解您的電腦，就可存取您的私人文件，利用您的電腦進行其惡意行為，甚至刪除重要的系統檔，讓您的電腦無法使用。

該應用程式是第一且最主要的防禦駭客程式，可根據安全策略 (一組規則) 控制您電腦上內送和外寄的流量。這些規則是在您安裝產品時所建立 (無論是自動或自我定義)。

應用程式的規則精靈會自動建立與存取 Internet 有關的應用程式行為規則。有經驗和沒有經驗的使用者有不同的模式，應用程式也有「伺服器模式知覺」功能。您可以建立和變更規則，並檢視流量和連接埠活動的詳細資訊。

此外，進階 Personal Firewall 提供：

- **啟動器保護，**
  - 可偵測到應用程式嘗試透過其他應用程式來啟動它自己。
- **暗中控制啟動保護，**
  - 可發現嘗試透過其他應用程式存取 Internet 的惡意應用程式。Personal Firewall 會追蹤所有的父系應用程式。
- **程序劫持保護，**
  - 可防止惡意應用程式劫持信任程序以注入 .dll 或執行緒。
- **完整的暗中控制模式，**
  - 可確保外部使用者完全無法看到您電腦上所有的連接埠。
- **進階 svchost 處理，**
  - 其中每一個 svchost 服務的規則與一般的規則不同，其規則可涵蓋每個 Svchost.exe 會話可包含的服務群組。
  - **Svchost** 是 Windows 2000/XP/2003/Vista 中服務的一般性主機程序名稱，各種網路與 Internet 程序皆可用以正確執行。此服務可以同時執行許多實例，每個實例都是操作個別電腦所必需的。此服務具有頻繁存取 Internet 之合法需求，與連線至網路的其他任何應用程式一樣，監控及警告此類活動屬於個人防火牆的工作。雖然許多防火牆在 svchost 處理方面只有一個一般規則，通常不可編輯，不過此個人防火牆可區分不同的實例，且可以識別程序為已知或未知。此外，應用程式的說明檔案中有一些 svchost 服務的配置選項。
- **防 pharming，**
  - 透過保護主機檔案來實施，因此可消除最常見的 pharming 攻擊方法。
  - **Pharming** 一詞是從網路釣魚 (phishing) 和寄養 (farming) 兩個名詞構建而來 (請參閱以下 Antispam 以取得網路釣魚的說明)。當駭客嘗試將流量從您即將造訪的網站重定向至另一個偽造網站時，便稱為 pharming。在目標電腦上變更主機檔案，或利用 DNS 伺服器軟體中的弱點皆可執行 pharming。DNS (網域名稱伺服器) 伺服器負責將 Internet 名稱解析至它們的真實位址。最近幾年，常見使用 pharming 與網路釣魚等方法來竊取線上識別資訊。Pharming 已經成為托管電子商務與線上銀行業務網站的企業最關心的事情。需要稱為防 pharming 的高級措施來阻止發生此嚴重威脅。

Antispam

Antispam 應用程式可阻止不必要的，且可能包含系統威脅之商務與大量電子郵件 (垃圾郵件)。Antispam 可阻止垃圾郵件、網路釣魚嘗試和其他電子郵件形式的威脅，不讓它們有機會侵擾電腦。您可以建立阻止及允許列表，來管理傳送電子郵件給您的發件者，及您允許送至電子郵件用戶端的內容。

就如同防毒應用程式運用病毒定義檔偵測惡意軟體一般，Antispam 解決方案使用定義檔篩選不必要的電子郵件。病毒定義檔含有決定檔案是否受感染的病毒特徵，而 Antispam 定義則使用一組條件判斷電子郵件是垃圾郵件的可能性。垃圾郵件定義檔是根據郵件所含的語言、圖片、色彩、連結以及寄件者的電子郵件與 IP 位址進行電子郵件分析。不過，這仍無法完全確定電子郵件是否為垃圾郵件。

- **垃圾郵件**
  - 不需要的電子郵件，通常都是某些產品的廣告。垃圾郵件一般都沒有害處，不過相當令人困擾，而且浪費時間。
- **釣魚欺詐**
  - 假裝是合法的公家機關或私人企業，將電子郵件傳送給某人，嘗試取得可用於身份竊取的私人資訊的動作。電子郵件會將您導引到要求您更新個人資訊的網站，例如信用卡及銀行帳號等實際的組織已擁有的資訊。這類網站當然是假的，但是看起來就像真的一樣，它的唯一目的就是竊取資訊。「網路釣魚」(phising) 一詞是從「釣魚」(fishing) 演變而來，隱含的意思就是誘使他人上鉤。

Parental Control

Internet 上的內容未必都是好的，有些網站是我們不想要讓兒童或青少年看到的。除非兒童和青少年隨時隨地受到監督，否則他們很有可能瀏覽到內容不宜網站 – 無論是故意或無心的。

有了 Parental Control，您可以阻止訪問某些類別的網站，甚至阻止所有未明確核准的網站。此外，您也可以限制允許使用者上網的時間，指定一天當中允許上網的時間。

簡言之，您可以根據年齡或其他您要考量的條件，為個別的使用者自訂配置檔案。

Privacy Tools

許多應用程式 (包括作業系統本身) 會記錄使用者活動，例如開啟的檔案、造訪的網站，以及檢視的文件等。這項使用者友好的機制可讓使用者輕鬆地執行重複的工作、造訪相同的在線報紙，或繼續處理文字文件。

雖然這可能是使用者友好的，但也會造成隱私上的顧慮。此電腦的其他使用者或後來檢查您電腦的其他人，可以檢閱這些日誌並探索您想要保有隱私的事。即使您將檔案從電腦中刪除，也不會完全清除該檔案。使用進階工具可找回檔案，從而入侵敏感性文件。日誌會追蹤您電腦上的 Internet 瀏覽和檔案開啟動作。

此功能與您的隱私緊密相關。它們會構成社交工程以及身份或密碼竊取的潛在風險。取得的個人資訊可進一步用於惡意目的。

您可以使用 Privacy Tools 來以安全的方式刪除特定檔案。檔案的內容會永久清除且無法復原。您也可以配置應用程式，使其自動刪除包含個人資料、cookie 和瀏覽器記錄的各種日誌檔案。刪除記錄日誌不會影響應用程式的設定與書籤。

Intrusion Guard

這是主機型入侵防範系統 (HIPS)，可以阻止惡意應用程式控制您的電腦。應用程式提供功能強大的報告工具，並保護程序、驅動程式、瀏覽器與主機檔案。它是專為有經驗的使用者設計並提供主動型執行緒保護的平台。

- 進階系統報告器工具
  - 此強大的工具可讓您控制在您電腦上發現的已安裝應用程式、系統篩選器以及可疑模組。
- 強大的即時功能
  - 此功能可配置為記錄、警告及阻止入侵。
- 程序保護
  - 阻止惡意應用程式劫持 (控制) 其他應用程式，及安裝更多惡意內容到您的電腦系統上。
- 驅動程式保護
  - 阻止驅動程式進行安裝，並防範其他惡意技術取得您電腦系統的低層級存取權。
- 瀏覽器劫持防護
  - 監控您的 Internet Explorer 設定並管理您的 cookie。也可以記錄、警告及阻止安裝網路篩選器的嘗試，例如 LSP (層次服務提供者) 和 BHO (瀏覽器幫助對象)。
- 主機檔案保護
  - 防止您的主機檔案遭到未經授權的修改。

安裝

以下章節包含系統需求、許可密鑰、如何檢索安裝程式，及如何在電腦上安裝 Norman Security Suite。

檢索軟體

當您購買 Norman Security Suite 時，會隨附含安裝程式的 CD，或者在購買文件上附有 Internet 下載的網頁位址。

CD-ROM

如果您收到來自 Norman 的 CD-ROM，請使用它來開始安裝。

1. 將 CD 放入 CD-ROM 光碟機。
   - CD 會自動執行，且 CD 功能表會顯示出來。如果 CD 功能表未在一分鐘左右之內出現，可能是已關閉「自動執行」功能。若要手動啟動 CD 功能表，請執行下列其中一項操作：
     - 瀏覽 CD 內容並連按兩下根檔案 Norman.exe。
     - 按一下**開始 > 執行**，然後輸入 D:\Norman.exe。以 CD-ROM 光碟機的實際分區代號取代 D:。按一下**確定**。
2. 選擇檢視 CD 功能表的語言。
3. 從 CD 功能表的**安裝**頁面選擇要安裝的語言。

會啟動 InstallShield Wizard。繼續參閱第 10 頁的「安裝」。

Internet 下載

您可以從 Internet 下載安裝程式。採購訂單資訊中已描述 Internet 位置與下載程序。如果沒有，請依照以下指示來下載安裝程式並開始安裝。

1. 開啟 Internet 瀏覽器，然後輸入 Norman 軟體下載的一般網址：
   http://www.norman.com/downloads/
2. 依據語言與/或版本選擇 Norman Security Suite 安裝程式。



注釋：根據您的 64 或 32 位元電腦選擇正確的安裝程式。

3. 按一下**儲存**或**執行**。

   a) **儲存**
   如果您按一下**儲存**，您便可在電腦上儲存檔案，及從該處開始安裝。當您從電腦安裝時，不需要 Internet 連線。但是，我們建議在安裝期間連線 Internet，以便進行密鑰驗證與更新。
   - 瀏覽要儲存安裝程式的資料夾位置，然後按一下**儲存**進行確認。
     - 記下您儲存安裝程式的位置。
     - 與下載視窗相同，不再需要瀏覽器，也可以將其關閉。
   - 尋找安裝程式並連按兩下檔案。
     - 成功安裝之後，可以刪除安裝程式，或者您可以將它儲存至外部媒體以供備份。

   b) **執行**
   按一下**執行**，直接從 Web 開始安裝。會下載安裝程式，然後立即開始安裝產品。如果安裝失敗，您必須再次造訪下載頁面。

會啟動 InstallShield Wizard。繼續參閱第 10 頁的「安裝」。

許可密鑰

當您購買 Norman Security Suite 時，會收到產品許可密鑰。更新安裝需要密鑰。未定期更新的防毒軟體無法達到其目的。

我有密鑰
安裝期間，您應該在收到 InstallShield Wizard 的提示時輸入密鑰。然後，應用程式將在安裝完成後自動搜尋更新。

我沒有密鑰
您可以將密鑰欄位保留空白，如此仍然可以安裝整個套裝軟體。但是，「授權精靈」會定期提示您輸入密鑰，否則將不會更新產品。

安裝完成後輸入密鑰
您可以從應用程式啟動「授權精靈」，然後將密鑰貼在適當欄位中。請參閱第 58 頁的「授權精靈」一節。

安裝

執行 Norman Security Suite InstallShield Wizard (安裝程式)。請參閱第 9 頁的「檢索軟體」，瞭解如何取得它。按照畫面上的指示進行操作。如果您需要檢查或變更安裝設定，請按一下**後退**。



安裝的預設位置為 `C:\Program Files\Norman`**。**

1. InstallShield Wizard 歡迎使用畫面會顯示出來。按一下**下一步**。
2. 閱讀授權合約並接受它以繼續安裝。按一下**下一步**。
3. 輸入有效的產品許可密鑰。按一下**下一步**。
   - 密鑰中含有您所購買產品的資訊。
   - 如果您只想評估產品，可以將欄位保留空白。我們建議您輸入試用密鑰，以在試用期充分利用產品。

提示

複製及貼上許可密鑰。如果您的許可密鑰是在電子郵件中或是其他電子格式，那麼最簡單的方法是將密鑰複製到許可密鑰欄位中。反白密鑰，按下 **Ctrl+C**，將游標放在許可密鑰欄位中，並按下 **Ctrl+V** 以貼上密鑰。確定未包含空白

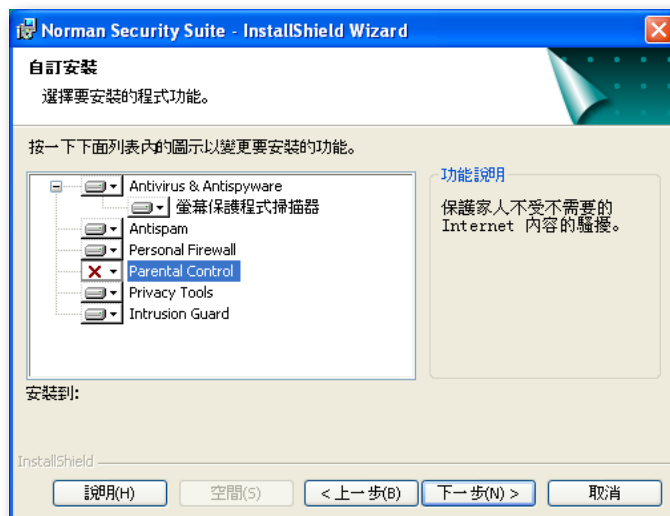


注釋：如果您沒有密鑰，可將此欄位保留空白，您仍然可以安裝整個套裝軟體。但是，「授權精靈」會定期提示您輸入密鑰，否則將不會更新產品。如果需要，「授權精靈」稍後將協助您取得密鑰。

4. **設定類型**
   a) 選擇**完整安裝**會將所有程式功能安裝至預設位置。
      - 選擇**完整安裝**並按一下**下一步**。
      - 繼續參閱以下的「7. 準備安裝。」。

   b) 選擇**自訂**可決定安裝哪些產品及/或選擇與預設位置不同的另一個位置。
      - 選擇**自訂**並按一下**下一步**。
5. **自訂設定**
   您可以安裝的產品列表會顯示出來。
   - **Antivirus & Antispyware**
     - **螢幕保護程式掃描器**
   - **Antispam**

- **Personal Firewall**
- **Parental Control**
  - 如果您要安裝本產品，需要手動選擇它。按一下左邊的下拉功能表，選擇在本機硬碟上安裝此功能。安裝本產品要求包括您的許可密鑰，或部分試用安裝。
  - 如果您願意，也可以稍後安裝本產品。
- **Privacy Tools**
- **Intrusion Guard**



◦ 如果您要查看所選安裝要求的磁碟空間，請按一下**空間**。
  - 按一下**確定**以返回至**自訂安裝**顯示。

◦ 按一下**下一步**繼續。

6. **目的地資料夾**

   a) 如果您要將所選應用程式安裝至預設位置，請按一下**下一步**。

   b) 按一下**變更 ...** 以定義其他位置。
   - 從下拉式列表中選擇位置、新增資料夾，或在資料夾名稱輸入欄位中輸入路徑。
   - 按一下**確定**，確認並返回至目的地資料夾顯示。
   - 按一下**下一步**。

7. 準備安裝。
   ◦ 按一下**安裝**，開始安裝。

8. 安裝 Norman Security Suite。
   ◦ 會顯示對話方塊，通知應用程式現在準備啟動及配置安裝的元件。按一下**確定**繼續。

9. 隨即顯示完成的對話方塊。按一下**完成**，完成 **InstallShield Wizard**。安裝將在背景下繼續執行 5-10 分鐘。

10. 當提示您重新啟動電腦時，按一下**立即重啟動**。重新啟動客戶註冊表單之後 (如果已安裝 Personal Firewall)，會啟動 Personal Firewall 安裝精靈。
    ◦ **客戶資訊**
      - 請輸入必要資訊，然後按一下**提交**。
    ◦ **安裝精靈**
      - 請參閱下一節。

精靈

Norman Security Suite 有三個不同的精靈。它們處理安裝及基本產品配置。

InstallShield Wizard

此精靈可讓您安裝 Norman Security Suite，亦稱為安裝程式或設定檔案。

安裝精靈

此精靈在安裝 Personal Firewall 時適用。安裝完含 Personal Firewall 的 Norman Security Suite 時，會啟動可供設定 Personal Firewall 的精靈。請參閱下一節。

授權精靈

此精靈會追蹤您的有效產品授權。請參閱第 58 頁的「授權精靈」一節。

安裝精靈

您已完成 Norman Security Suite 安裝 (參閱第 10 頁的「安裝」)，Personal Firewall 是已安裝的其中一項功能。會自動啟動安裝精靈。

此精靈會自動建立基本規則，例如允許相關應用程式訪問 Internet。目的是找出訪問 Internet 之需求為合法的程式，並為這些應用程式建立規則。強烈建議您執行安裝精靈。您可以隨時使用「規則編輯器」，於日後變更自動產生的規則。

如果您選擇不執行「安裝精靈」，可能會發現電腦無法連線至 Internet，且不會更新重要的應用程式。請參閱第 58 頁的「授權精靈」一節。

1. 閱讀簡介頁並按一下**下一步**。
   「安裝精靈」會針對有經驗與沒有經驗的使用者提供不同的步驟。有經驗的使用者可以指定某些詳細資訊，而沒有經驗的使用者可由自動配置引導。
2. 請評估自己的經驗等級並按一下**下一步**。

   沒有經驗的使用者

   ◦ 您是一位非專業或對電腦技術方面不感興趣的普通 Internet 使用者。防火牆將為您做出幾個決定，您與程式之間的互動將盡可能減少。
   ◦ 選擇安全等級，以便處理嘗試存取電腦 (內送) 的 Internet 連線，或嘗試連線至 Internet (外發) 的應用程式。
     • **基本模式**。
       - 除非永久規則阻止連線，將允許所有流量。這將使您能夠防範內送攻擊。
     • **正常模式**。
       - 除非永久規則阻止連線，否則系統會提示您有未知流量，以及是否要允許或拒絕該流量。這將使您能夠防範內送攻擊以及從您的電腦傳出資料的非所需應用程式。

   有經驗的使用者

   ◦ 您熟悉通用防火牆設定，而且懂得什麼是 IP 位址與連接埠號。防火牆在設定及使用期間會提供更多進階選項。
3. 按照畫面上的指示，新增其他 Web 瀏覽器或電子郵件用戶端、配置網路資源 (如果選擇有經驗的使用者，則為進階配置)，及允許其他已知應用程式。
4. 最後，按一下**完成**以完成精靈。

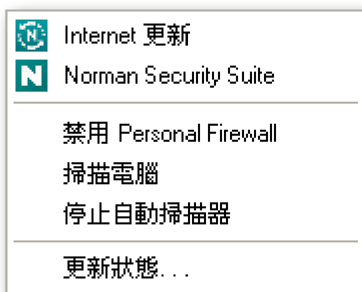
入門

應用程式托盤圖示

設定時，圖示會出現在畫面右下角的系統托盤中。此圖示確認 Security Suite 已安裝在此電腦中。



在托盤圖示上按一下滑鼠右鍵會顯示 Security Suite 系統托盤功能表。



在列表中，前面標記圖示的項目是該項目的複本，這些複本出現在**開始 > 程式集 > Norman Security Suite** 功能表中。這是 Norman Security Suite 主模組以及一些一般工作的捷徑。

- **Internet 更新**
  - 啟動「Internet 更新」功能並更新安裝的產品。
- **Norman Security Suite**
  - 開啟 Norman Security Suite 應用程式。
- **禁用 Personal Firewall (啟用 Personal Firewall)**
  - 在啟用及禁用 Personal Firewall 之間切換。
- **掃描電腦**
  - 開始手動掃描整台電腦。
- **停止自動掃描器 (啟動自動掃描器)**
  - 在啟動與停止自動掃描器之間切換。
- **更新狀態 ...**
  - 檢視已安裝產品的更新狀態。此功能也是過時病毒定義檔、授權到期和其他相關資訊的訊息起源。



注釋：功能表選項根據安裝的產品而有所不同。例如，只有安裝了 Personal Firewall，才能看見「啟用 Personal Firewall」或「禁用 Personal Firewall」選項。

托盤警告圖示

托盤圖示也提供與 Security Suite 安裝狀態相關的資訊。請將游標置於托盤圖示上，以瞭解任何錯誤或訊息的說明。

紅色圓圈



此圖示表示一些目前正在執行的元件已過時。如果圖示旁有閃爍的紅色符號，請將指標放在該符號上以找出需要更新的元件，或是否有其他錯誤狀況。

注釋：在啟動期間可看見紅色符號，直到所有模組啟動為止。若電腦較舊且速度較慢，則載入所有模組的時間較長。但是，正常 Norman 圖示最慢應在 2 分鐘後出現

黃色三角形



靜止或閃爍的黃色三角形圖示表示已手動禁用自動掃描器、應用程式正在等待重新啟動、發生安裝錯誤，或者定義檔已過時。

- **靜止**
  - 已在應用程式的設定中手動禁用自動掃描器。請參閱第 23 頁的「啟用自動掃描器」。
  - 應用程式正在等待重新啟動。可能已經在出現上一個提示時選擇**稍後重新啟動**選項。
  - 發生可能的安裝錯誤。嘗試重新啟動電腦，以解決可能的錯誤。
- **閃爍**
  - 病毒定義檔已過時。這表示它們至少已有十天之久。
  - 已從系統托盤功能表中停止自動掃描器。在系統托盤圖示上按一下滑鼠右鍵。選擇**啟動自動掃描器**。
  - 已禁用防火牆。在系統托盤圖示上按一下滑鼠右鍵。選擇**啟用 Personal Firewall**。

黃色齒輪



當托盤圖示旁出現齒輪時，Norman 程式管理員會操控該程式，最可能為執行更新。不建議您在 NPM 運作 (也就是看得到此符號) 時關閉電腦。

注釋：更新時間不應超過 5-10 分鐘。如果齒輪圖示出現時間超過 5-10 分鐘，表示該安裝有錯誤。如果遇到這種情況，請嘗試重新啟動電腦。如果重新啟動電腦之後齒輪圖示仍然存在，請嘗試使用修復選項，如第 61 頁的「自動修復」一節所述。

Windows 資訊安全中心符號



Norman 是作業系統偵測到的其中一個防毒軟體供應商。如果病毒定義檔過時，或未執行自動掃描器，或者已禁用防火牆，您也會收到 Windows 表示發生錯誤的警告。「資訊安全中心」符號出現，您可以按一下該符號來檢視與編輯 Windows 設定。

開啟應用程式

您可以使用系統托盤功能表或 Windows 功能表開啟應用程式。在應用程式的系統托盤圖示上按一下滑鼠右鍵，並從快顯功能表中選擇 **Norman Security Suite**。從 Windows 功能表中，按一下**開始**並選擇**所有程式 > Norman Security Suite > Norman Security Suite**。

產品警告圖示

有時，黃色三角形會顯示在應用程式的功能表項目上。出現此符號的可能原因是，產品遭禁用或過期、許可證過期、新安裝的軟體需要最終的配置才能完成其安裝程序等等。請選擇包含警告的功能表項目，瞭解詳細資訊。



注釋：當您第一次開啟 Security Suite 時，會針對 Parental Control 應用程式發出警告。**請參閱第 44 頁的「Parental Control」一節**

Security Suite 設定

此應用程式以我們針對每天使用建議的預設設定安裝。您可以從應用程式的主產品頁中選擇**自訂設定**，透過一些不同選項配置產品。當從一個設定變更為另一個設定時，請注意圖示的變化，且設定會導致文字位置變化。



- 目前設定：**建議**
  - 預設設定有效，建議每天使用。
  - 如果您要變更預設設定，請按一下**自訂設定**。

- 目前設定：**自訂**
  - 預設設定為自訂，或者可以自訂。
  - 按一下**使用建議的設定**，將設定重設為預設值。



注釋：除非您瞭解變更會對系統造成的影響，否則不建議變更預設設定。請確定自訂設定不會導致較低的安全等級。如果您不確定，請記住，預設設定可以提供足夠的保護

首頁

開啟 Security Suite 應用程式，檢視已安裝產品的狀態。關於開啟應用程式的方法，請參閱第 13 頁的「入門」。



掃描您的電腦，追蹤已安裝的產品、它們的狀態，及檢視其相關詳細資訊。更新所有產品，並按一下滑鼠鍵來開啟或關閉自動更新。

按一下**掃描電腦**，開始手動掃描整部電腦。此掃描使用的設定與為手動掃描器所指定的設定相同。請參閱第 25 頁的「手動掃描器」。

授權的產品是產品許可密鑰所涵蓋的產品。請參閱第 10 頁的「許可密鑰」。狀態圖示會指示安裝是否為最新以及是否完全 (若需要更新)，或是否未安裝某產品。右側的統計資訊顯示運作中應用程式的資料。



注釋：當您第一次開啟 Security Suite 時，會針對 Parental Control 應用程式發出警告。請參閱第 44 頁的「Parental Control」一節

更新全部的產品

只需按一下滑鼠鍵，即可更新所有安裝的產品。如需詳細設定與概觀，請參閱第 57 頁的「安裝和更新」。

自動更新開啟/關閉

開啟自動更新後，產品將會定期更新。在第 58 頁的「選擇更新方式」中編輯設定。



注釋：我們強烈建議您始終開啟自動更新

Antivirus & Antispyware

開啟 Security Suite 應用程式，並從左側功能表中選擇 **Antivirus & Antispyware**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」；關於應用程式的目的與功能說明，請參閱第 5 頁的「Antivirus & Antispyware」。

主頁面



此防毒與反間諜軟體應用程式可監控您的個人電腦是否有惡意軟體。本章介紹如何配置兩種主要病毒掃描器：自動掃描器與手動掃描器，以及如何管理被隔離的檔案、排程掃描、啟動螢幕保護程式掃描器及啟用反間諜軟體功能。

自訂設定

按一下此選項可編輯預設值。請參閱第 22 頁的「設定」。關於選擇建議及自訂設定的一般資訊，請參閱第 15 頁的「Security Suite 設定」。

掃描統計資訊

應用程式的主頁面會以圖形表示方式顯示過去 24 小時內已掃描的檔案及已感染病毒的檔案。統計數字反映手動與自動掃描器的聯合動作。

爆發模式

只有在發生病毒爆發以及連線到未知或不安全的無線網路時，才應該暫時啟動此功能。啟用此選項可能會影響效能與穩定性。

停用自動檔案掃描

請參閱第 23 頁的**設定 > 自動掃描器**一節。

掃描電腦
這是手動掃描器，它會啟動對系統中所有硬碟的掃描。您可以從顯示的掃描對話方塊中，選擇**停止**（若您想要**瀏覽**另一個要掃描的位置）。按一下**開始**，繼續手動掃描會話。

您也可以從系統托盤功能表啟動此掃描。在應用程式的托盤圖示上按一下滑鼠右鍵，並選擇**掃描電腦**。

關於如何配置手動掃描器的資訊，請參閱第 25 頁的「手動掃描器」。

隔離區

Antivirus & Antispyware > 隔離區　說明

目前設定: 建議　自訂設定

將檔案保留在隔離區

最小值 2天　最大值 2 周

隔離區的最大空間 (分區的 %) 10%

儲存

被隔離的檔案

檔案名	診斷	日期	儲存至
沒有供顯示的專案。			

全部選擇　還原　刪除　重新整理檢視

將檔案保留在隔離區

選擇**自訂設定**，存取配置選項。指定檔案存放在隔離區的最短時間和最長時間，以及允許它們佔用多少磁碟空間。

- **最小值**
  指定從一天到一週的一個時間段。從不刪除未超過此指定最短時間的檔案。
- **最大值**
  指定從一週到四週的一個時間段。超過這段最長時間的檔案將被直接刪除，不會發出任何警告提示。
- **隔離區的最大空間（分區的 %）**
  指定允許被隔離檔案佔用目前分區的多少磁碟空間。



注釋：如果被隔離的檔案尚未達到指定的最短時間，就可以超過最大空間的限制

- 按一下**儲存**確認變更。

被隔離的檔案

如果您已將程式配置為：將被隔離的感染檔案在**被隔離的檔案**對話方塊中顯示為列表，則會如此顯示。防毒應用程式在刪除或隔離感染的檔案之前，會先嘗試修復感染的檔案（視配置而定）。被隔離的檔案是感染的檔案，或已由「Internet 保護」功能阻止的檔案。



注釋：預設會將被刪除或阻止的檔案複本隔離。

除非被感染和被隔離檔案的複本位於其他資料夾中（在這種情況下，會將其移至隔離區），否則該複本會遭到刪除。自動掃描器偵測到 C:\eicar.com 感染時，會將檔案移到隔離區。但是，如果自動掃描器偵測到 C:\eicar.com 複本，且此檔案與 eicar.com 相同，則不會隔離它，但會將它刪除。但如果 eicar.com 複本位於 C:\ 其他資料夾 \ 中，則因為它位於新位置的緣故，所以會將此檔案移到隔離區。實施此方法的目的是為了避免病毒將同一個檔案的多份複本寫入磁碟機的同一個位置上，而塞爆隔離區。

由於 Antivirus 應用程式懷疑檔案被感染，該檔案可能會被隔離。在少見情況下且在定義檔更新之後，Antivirus 應用程式會確定先前被隔離的檔案究竟是否清潔無毒。由於用於製作及偵測病毒的類型和技術都快速變化，因此 Antivirus 應用程式會在更新及電腦重新啟動之後掃描隔離區。

如果被隔離的檔案在經過此類檢查後獲「無罪釋放」，便會還原該檔案，但前提是具有有效的檔案路徑，且不存在其他名稱相同的檔案。不需要使用者介入，且不會告知您可能會還原被隔離的檔案。

工作編輯器

有時，定義應多次及/或定期執行的工作會很方便。掃描病毒是一項需要定期執行的工作的典型實例，「工作編輯器」則是可用於達成該目的的工具。

對於要重複執行的掃描，或是要在特定情況下執行的特殊掃描，您可以建立工作檔案。例如，若您從 Internet 下載檔案至指定區域，您可以建立只掃描這些區域的工作檔案，並在下載後手動執行該工作。此外，您可將該工作排程為於預先選取的時間執行。

管理員可以建立工作檔案，並將它們發佈至網路中的所有工作站，以確保對需要特殊注意的區域執行一致性檢查。



注釋：在您第一次存取工作編輯器時，或尚未建立任何工作時，會顯示建立一項工作對話方塊。

所有現有工作會顯示於「工作編輯器」對話方塊內的列表中。

建立一項工作

Antivirus & Antispyware > 工作編輯器　說明

建立一項工作

工作名稱

掃描整台電腦　掃描所選擇的檔案與資料夾

新增

掃描引導區
掃描歸檔
掃描記憶體

排程要執行的掃描

每日　2010-04-30　13:45

已啟用

建立　取消

1. 輸入**工作名稱**。
2. 選擇**掃描整台電腦**或**掃描所選擇的檔案與資料夾**。
   - 按一下資料夾搜尋符號可瀏覽檔案或資料夾。
     - 採用類似 Windows 檔案總管的功能列出所有本機磁碟。
     - 按一下磁碟號即可瀏覽目錄或檔案。
     - 如果選擇了特定的檔案與資料夾，所選磁碟/資料夾下的子資料夾都將自動被核取。您可以清除您不想包含的子資料夾的選項。
   - 也可以直接在輸入文字欄位中輸入路徑以及檔案或目錄名稱。
     - 也接受星號通配符 (*)，例如，C:*.* 將對整個 C: 碟進行掃描。
     - 將通配符置於搜尋字詞開頭或結尾。請勿將通配符置於搜尋字詞中間。
   - 按一下**新增**進行儲存時，指定的區域會新增到工作列表中。
3. 選擇一個或多個掃描選項。**掃描引導區**、**掃描歸檔**和**掃描記憶體**都已預先選擇。除了這些，還會使用手動掃描器的掃描選項。
   - **掃描引導區**
     - 如果選擇此選項，Antivirus & Antispyware 應用程式將檢查所掃描區域的引導區。
   - **掃描歸檔**
     - 如果選擇該選項，在掃描中包含已歸檔的檔案。目前支援如下格式：ACE、APPLE_SINGLE、ARJ、BZIP2、CAB、GZ、LZH、MAIL、RAR、RAR3、SFXZIP、TAR、ZIP 與 7Z。
   - **掃描記憶體**
     - 掃描記憶體區時，Antivirus & Antispyware 應用程式將搜尋駐留病毒。您務必確保記憶體中沒有病毒。

排程要執行的掃描

4. 選擇要執行掃描的頻率、時間和日期。建議的日期與時間就是目前的日期與時間 （依照系統資訊）。您可以選擇其他時間。
5. 掃描工作預設為**已啟用**。移除勾號以禁用它。

6. 按一下**建立**。



所有排程的工作會顯示於**工作編輯器**對話方塊內的列表中。您可以在「工作編輯器」對話方塊中檢視、編輯、執行及刪除工作檔案。您可以在這裡啟動及停用或刪除工作。取消選擇**活動**核取方塊可停用工作。選擇**刪除**核取方塊並按一下**刪除所選**可刪除工作。

儲存工作檔案的預設位置為 `...Program Files\Norman\Tasks`。

移除工作

若要移除工作，請選擇工作列表中的一個或多個項目，然後按一下**刪除所選**。

排除列表



不會掃描位於排除列表之上的檔案。不掃描某些檔案的理由是這些檔案會觸發錯誤的警報，或是掃描這些檔案會花費太多的時間。無論出於什麼原因，我們都建議您定期執行計劃掃描或手動掃描，對排除列表上的檔案進行掃描。



注釋：應該謹慎對待排除列表，因為它們代表的是潛在的安全風險。請注意：不對檔案或區域進行掃描是一項以犧牲安全性為代價的決定。

使用排除列表

選擇該選項以啟動排除列表。**排除列表**用於排除可能與掃描器出現衝突的檔案，會影響電腦的性能。

不對某些檔案與資料夾進行掃描

請指定不需要進行惡意軟體掃描的檔案、目錄或整個磁碟。請按如下步驟來選擇不掃描的內容：

- 若您要瀏覽檔案和資料夾，請按一下資料夾搜尋符號，或在輸入欄位中輸入檔案名稱、目錄或磁碟機代碼。

  通配符 (*/?) 也接受。將通配符置於搜尋字詞開頭或結尾。請勿將通配符置於搜尋字詞中間。

注釋：指定要排除的內容時請勿使用撇號 (“ 或 ‘)。

示例

C:\Dir	排除目錄與子目錄下的所有檔案
*.xyz	排除副檔名為 .xyz 的所有檔案
example.exe	排除指定的檔案，無論從何處找到
C:\System\xyz.doc	排除此特定的檔案

- 指定哪些掃描器 (如果有的話) 應該使用排除列表。
- 隨後按一下**新增至列表**，將內容新增到排除列表中。

注釋：Security Suite 不會檢查已加入到排除列表中的檔案、資料夾或磁碟機是否已存在。請務必輸入正確的名稱和路徑。

網路磁碟

如果您不想掃描可在遠端電腦上存取的共用檔，您可以排除網路磁碟。指定所針對的掃描器 (如果有的話)。

刪除所選

若要將項目從排除列表中移除，請選擇項目，並按一下**刪除所選**。按一下**儲存**確認變更。

注釋：我們建議您定期修改排除列表。

設定

您可以在此部分配置自動掃描器、手動掃描器以及「Internet 保護」功能。自動與手動掃描器預設都使用 Norman Sandbox。詳情請見第 63 頁的「何謂 Sandbox？」中的 Sandbox。對於**掃描電腦**選項、右鍵掃描器、螢幕保護程式掃描器及指令行掃描器來說，手動掃描器設定也是相關的。

自動掃描器

自動掃描器在背景作業，會自動保護您的系統。它是一個很重要的病毒控制元件，因此應該隨時啟用。



啟用自動掃描器

選擇/取消選擇此選項即可啟動和停止自動掃描器。建議隨時啟用自動掃描器。



如果使用托盤功能表來停止或暫停自動掃描器，則會在系統托盤圖示中顯示閃爍的黃色三角形。請參閱第 13 頁的「應用程式托盤圖示」。此外，「Windows 資訊安全中心」還將警告您：「您的電腦可能存在風險」。

1. 在「自動掃描器設定」功能表中，確定已選擇**啟用自動掃描器**選項。按一下**儲存**確認變更。
   - 清除此核取方塊可禁用自動掃描器。
   - 如果您用這種方法禁用自動掃描器，Norman Security Suite 不會發出警告。但是，Windows 的「資訊安全中心」會發出警告。



注釋：清除啟用自動掃描器核取方塊表示，在手動重新啟用自動掃描器之前，它會保持禁用狀態。

2. 在系統托盤功能表中按一下**啟動自動掃描器**。
   - 此選項會在**啟動自動掃描器**與**停止自動掃描器**之間切換。
   - 如果手動停止掃描器，它將會於下次重新啟動電腦或安裝 Security Suite 更新時啟用。

自動移除偵測到的病毒

掃描器會偵測並移除所有類型的病毒。儘可能先修復中毒的檔案，再將檔案交給應用程式。如果修復失敗，則拒絕存取中毒的檔案。請注意：如果檔案僅僅包含惡意軟體，它將被整個刪除掉。

使用者模式

使用者模式部分分為兩個模組：「本機使用者」和「服務與遠端使用者」。在正常情況下，工作站會在**本機使用者**模式下執行，而伺服器則會在**服務與遠端使用者**模式下執行。預設設定可在大部份情況下提供充分保護，因此除非您十分清楚可能的結果，否則不建議變更預設設定。

本機使用者

- **讀取/執行**
  - 指示自動掃描器在使用檔案前掃描檔案。
  - 示例：當使用者連按兩下 .doc 檔案時，自動掃描器會檢查檔案以及啟動的應用程式 (在此情況下為 MS Word)。
- **讀取與寫入時皆掃描**
  - 指示自動掃描器掃描已開啟供寫入的檔案，例如當使用者從 Internet 下載檔案時。
  - 若您選擇於**讀取/執行**時掃描，就可能會下載中毒的檔案並儲存至磁碟。不過，自動掃描器會在您嘗試開啟檔案時偵測病毒。

服務與遠端使用者

此模式適用於任何已登出的 XP/Vista/Windows 7 電腦，且該電腦理論上可當作伺服器使用。您可於此處選擇是要在使用檔案前及/或建立新檔案時掃描檔案，還是在變更現有檔案時掃描檔案。換言之，您是選擇自動掃描的策略，該策略會在您從 Internet 或 FTP 伺服器儲存下載的檔案時生效，或在其他電腦將檔案寫入您電腦上的網路共用時生效。

- **寫入**
  - 指示自動掃描器掃描儲存至磁碟的檔案，例如當使用者要將檔案儲存在伺服器時。在此情況下，伺服器上的自動掃描器會掃描檔案。
- **讀取與寫入時皆掃描**
  - 這可能是您不需要的選項。此選項在一種情況下會很有用，即伺服器受到感染時，例如由於缺少掃描器更新而導致感染。在此情況下於讀取與寫入時皆掃描，將可防止感染經由網路進一步散佈。

使用 Sandbox

Sandbox 功能用來偵測新的不明病毒。如果希望掃描器留意新的病毒變體，則請選擇該選項。該 Sandbox 專門針對新郵件、網路以及對等蠕蟲及檔案病毒，同時還對不明安全威脅起作用。

- **已禁用**
  - 已關閉 Sandbox 功能。
- **標準**
  - 建議的掃描層級。當此選項啟用時，Sandbox 會檢查本機使用者和遠端/服務的所有寫入作業。
- **已延期**
  - 您可以在重大情況下選擇此模式，例如當您的系統爆發病毒，且在有限期間內沒有以簽名為基礎的偵測可用時。Sandbox 便會在讀取以及執行時皆檢查。如果選擇該選項，掃描時間會增加，但不會對系統性能造成過大的影響。

按一下**儲存**確認變更。

手動掃描器

使用手動掃描器掃描您電腦上的所選區域。掃描整個硬碟會消耗太多的時間。如需定期掃描整個磁碟機、選擇的資料夾或檔案，建議您設定排程掃描。使用「工作編輯器」並啟用螢幕保護程式掃描器，以便在活動少或空閒的期間自動執行手動掃描。最後，您可以在檔案系統物件上按一下滑鼠右鍵，啟動手動掃描器。所有這些掃描方式都採用手動掃描器的設定。



使用 Sandbox

Sandbox 功能用來偵測新的不明病毒。如果希望掃描器留意新的病毒變體，則請選擇該選項。該 Sandbox 專門針對新郵件、網路以及對等蠕蟲及檔案病毒，同時還對不明安全威脅起作用。如果選擇該選項，掃描時間會增加，但不會對系統性能造成過大的影響。

自動移除偵測到的病毒

應用程式試圖從被感染檔案中移除病毒。選擇該選項以自動修復被感染的檔案。除了引導區病毒外，大多數病毒都可即時移除。提示使用者干預總是先於引導區病毒的移除。請注意：如果檔案僅僅包含惡意軟體，它將被整個刪除掉。

掃描歸檔

如果選擇該選項，在掃描中包含已歸檔的檔案。目前支援如下格式：ACE、APPLE_SINGLE、ARJ、BZIP2、CAB、GZ、LZH、MAIL、RAR、RAR3、SFXZIP、TAR、ZIP 與 7Z。

記錄

- **建立日誌檔案**
  每次執行手動掃描時均在 C:\Program Files\Norman\Logs 資料夾下建立一個日誌檔案。如果取消選擇該選項，手動掃描時就不會生成日誌檔案。預設情形下啟用該選項。
- **詳細記錄**
  生成一份詳細報告，指定被掃描的每個檔案、每個檔案的掃描時間、狀態等。

Internet 保護

此篩選器可防止病毒經由 Internet 電子郵件和新聞讀取器散佈。目前已通報的病毒中，有絕大部分會使用讓自己經由電子郵件散佈的機制。此篩選器模組是專為攔截內送和外寄的郵件和新聞所設計，且會移除或阻止所有感染附件的不當內容。它不但能掃描電子郵件中的已知病毒，還可根據內容和檔案副檔名阻止檔案附件。

Antivirus & Antispyware > 設定　說明
目前設定: 建議　自訂設定
自動掃描器　手動掃描器　Internet 保護
使用 Sandbox
要掃描的流量
內送電子郵件
外寄電子郵件
新聞群組
即時傳送（接收的檔案）
阻止附件
阻止所有附件
阻止帶雙副檔名的檔案
阻止 CLSID 檔案類型的附件
阻止加密附件

附件列表
阻止下列所有附件
阻止下列附件外的所有附件
逗號分隔列表。範例：evilattachment.exe、*.pif、*.dll
連接埠
110 內送電子郵件 (POP3)
25 外寄電子郵件 (SMTP)
119 新聞群組 (NNTP)

使用 Sandbox

Sandbox 功能用來偵測新的不明病毒。如果希望掃描器留意新的病毒變體，則請選擇該選項。該 Sandbox 專門針對新郵件、網路以及對等蠕蟲及檔案病毒，同時還對不明安全威脅起作用。如果選擇該選項，掃描時間會增加，但不會對系統性能造成過大的影響。如需 Sandbox 的詳細資訊，請參閱第 63 頁的「附錄 A」。

要掃描的流量

選擇希望對 Internet 流量的哪些元素進行掃描。預設為全部掃描。

- **內送電子郵件 (POP3)，**
  - 對他人傳送給您的所有電子郵件進行掃描。而且，即使是您最親密的朋友或者最親近的業務夥伴也可能會無視病毒感染。
- **外寄電子郵件 (SMTP)，**
  - 對您傳送的所有電子郵件進行掃描。如果電腦感染了惡意軟體而您又沒有意識到，您就可能無意間給朋友或業務夥伴傳送被感染的郵件。
- **新聞群組 (NNTP)，**
  - 對在您的電腦與您參與的群組/論壇的其他使用者之間產生的流量進行掃描。
- **即時傳送 (接收的檔案)，**
  - 掃描 MSN Messenger 與 Windows Messenger 的即時傳送期間的檔案傳輸流量。選擇該選項後，就將掃描內送的檔案是否被惡意軟體感染。如果檔案已感染，則會彈出快顯訊息警告發生此事件。
  - 此功能只會掃描檔案傳輸，所以感染的連結仍會帶來威脅。



請注意：當被傳輸的檔案寫入目錄 ...\Temporary Internet Files **時，系統對它們進行掃描。如果偵測到惡意軟體，就可能要隔離一個 TMP 檔案。如要還原被隔離的 TMP 檔案，請選擇必要的檔案，並從右鍵按一下功能表選擇**儲存為**選項，使用原始檔案名與副檔名儲存檔案。****請參閱第 18 頁的「隔離區」。**

阻止附件

該功能在電子郵件蠕蟲病毒蔓延、且蠕蟲病毒可以按檔案名識別時尤其有用。阻止附件功能對於阻止您不希望進入您的郵箱的檔案類型也非常有用。附件被阻止後，將被移動到隔離區，而不是被刪除掉。您可以輸入確切的資訊，按名稱或副檔名阻止附件。這是可用配置選項的簡短說明：

- **阻止所有附件**
  - 所有附件均被阻止。
- **阻止帶雙副檔名的檔案**
  - 許多蠕蟲以及電子郵件病毒都套用了新增附加副檔名這樣一項技巧，如 **Filename.jpg.vbs**。許多電子郵件用戶端均隱藏後面的副檔名，因而造成附件只帶一個副檔名 JPG 的假像。但是，這個功能不只有病毒會使用 – 檔名如 **Myfile.hlp.zip** 和 **Todolist_20.dec.doc** 這類的合法檔案也會被視為雙重副檔名。
- **阻止 CLSID 檔案類型的附件**
  - 有些最新的蠕蟲以及電子郵件病毒套用 CLSID 技巧來欺騙電子郵件掃描器以及具有阻止功能的軟體。它們利用 Windows 中的功能，將 .exe 副檔名取代成為 {...} 副檔名，因而逃避對 EXE 檔案的阻止。正統的附件沒有理由來使用這種副檔名，因此，預設情形下系統即阻止這種行為。
- **阻止加密附件**
  - 取決於所用工具，同普通檔案附件相比，掃描壓縮與加密檔案是否感染了病毒一般更為困難。因此，防毒應用程式提供了徹底阻止此類附件的選項。

附件列表

使用該功能來明確選擇您希望阻止或者接受的附件。您可以輸入確切的附件名，或者使用通配符 (*) 來阻止某些副檔名。內容隨即出現在列表框中，您以後可以從中對它進行編輯或者把它移除。

例如，輸入 `*.exe` 可阻止或允許具有 EXE 副檔名的所有附件。將通配符置於搜尋字詞開頭或結尾。請勿將通配符置於搜尋字詞中間。

- **阻止下列所有附件**
  - 所有您**儲存**至列表的名稱都會被**阻止**。
  - 按一下**儲存**進行確認
- **阻止下列附件外的所有附件**
  - 所有您**儲存**至列表的名稱都會被**接受**。
  - 按一下**儲存**進行確認



注釋：請注意：仔細區分這兩個選項非常重要，因為它們分別代表兩個極端：即阻止列表上的所有內容或者接受列表上的所有內容。

如需有關此主題的詳細資訊，請參閱應用程式的說明檔案。

移除項目

選擇一個或多個項目，並按一下**移除所選專案**。按一下**儲存**進行確認。

連接埠

在眾多用於電腦之間通訊的通訊協定中，有一些是使用 Internet 時必要的。為了統一標準，已事先為通訊協定指定好連接埠號。

連接埠號

用於電腦通訊的某些協定對於 Internet 的使用非常重要。為了統一標準，已事先指定好連接埠號。您已在「要掃描的流量」部分中，選擇了您想要掃描的 Internet 流量。本對話標識了傳送與接收電子郵件需要的協定，以及根據行業標準，電腦上所對應的連接埠號。

您可能已給此處列出的一個或多個支援的協定指定了不同的連接埠號。在這種情形下，您必須輸入涉及到的協定的實際連接埠號。

下面的協定是目前支援的協定。必要時系統將更新此表。對話中指定的連接埠號與功能包括：

- **內送電子郵件 (POP3)**
  (連接埠 110) POP 是郵局通訊協定 (Post Office Protocol) 的縮寫。
- **外寄電子郵件 (SMTP)**
  (連接埠 25) SMTP 是簡易郵件傳送通訊協定 (Simple Mail Transfer Protocol) 的縮寫。
- **新聞群組 (NNTP)**
  (連接埠 119) NNTP 是網路 NEWS 傳輸通訊協定 (Network News Transfer Protocol) 的縮寫。

其他掃描方式

啟用螢幕保護程式掃描器

如果您選擇螢幕保護程式掃描器，則會在空閒期間執行系統的病毒掃描。閒置時間就是系統處於非活動狀態的一段時間，即沒有鍵擊、沒有滑鼠移動。

螢幕保護程式一旦啟動，手動掃描器便會開始掃描所有硬碟。啟動電腦後 (例如透過移動滑鼠或按下鍵盤按鍵)，螢幕保護程式掃描即會中止。如果掃描未完成，則下次啟動掃描時，會從停止掃描之處繼續掃描。

1. 移至 **Antivirus & Antispyware**，並選擇**啟用螢幕保護程式掃描器**。
    - Windows 控制台的「顯示內容」對話方塊會出現。



2. 從**螢幕保護程式**下拉式列表中選擇 **Norman 螢幕保護程式**。
    - 按一下**如果想要請預覽**查看啟動的螢幕保護程式。
    - 移動滑鼠或按下鍵盤按鍵可中止預覽。
3. 按一下**確定**確認變更。

下次系統閒置且啟動「Norman 螢幕保護程式」時，手動掃描器即會開始掃描硬碟，並不斷顯示進度。移動滑鼠或按下鍵盤按鍵可中止「螢幕保護程式掃描器」。



注釋：螢幕保護程式掃描使用的設定與為手動掃描器所指定的設定相同。

按一下滑鼠右鍵以進行掃描

這是手動掃描器，透過 Windows 的右鍵快顯功能表開始掃描所選檔案或資料夾。

- 在檔案或資料夾上按一下滑鼠右鍵。
    - 例如，在 Windows 檔案總管中或在桌面上。
- 從快顯功能表選擇**掃描有無病毒**。
- **手動掃描器**對話方塊會出現。您可以**瀏覽**另一個要掃描的檔案或資料夾，並**開始**、**暫停**或**停止**掃描程序。

指令行掃描器

「指令行掃描器」是 GUI 掃描器的替代方法，讓使用者可從指令行執行批次作業和其他掃描工作。指令行掃描器對於熟悉此環境的人而言是很好的替代方法。

指令行掃描器的基本功能與功能表式掃描器相同，獨立於其他模組。它也可以從批次檔案執行。

啟動指令行掃描器

1. 開始指令提示會話。
   - 移至**開始** > **執行**。
   - 輸入 CMD，並按一下**確定**或按 **Enter**。
2. 移至 Antivirus & Antispyware 應用程式所在的目錄。
   - 預設位置為 `C:\Program Files\Norman\nvc\bin\`
3. 輸入所需參數並按 Enter。
   - 如需可用參數的列表，請輸入：

     ```
     nvcc /?
     ```
   - 語法為：

     ```
     nvcc [磁碟機]:[路徑] [/參數] [Enter]
     ```
   - 使用的每個參數之前必須留空格。

Personal Firewall

完成安裝精靈 (請參閱第 12 頁的「安裝精靈」)。開啟 Security Suite 應用程式，並從左側功能表中選擇 **Personal Firewall**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」；關於應用程式的目的與功能說明，請參閱第 6 頁的「Personal Firewall」。關於初始化 Personal Firewall 的方法，請參閱第 12 頁的「安裝精靈」。

主頁面



本章主要介紹如何配置防火牆應用程式、建立可控制內送與外發應用程式的規則、檢視流量等。應用程式可區分沒有經驗和有經驗的使用者。沒有經驗的使用者會由安裝精靈進行引導，而有經驗的使用者則可執行進階設定的詳細配置。

自訂設定

按一下此選項可編輯預設值。請參閱第 39 頁的 Personal Firewall「設定」。關於選擇建議及自訂設定的一般資訊，請參閱第 15 頁的「Security Suite 設定」。

統計資訊

統計資訊會顯示已阻止的內送和外寄連線與連接埠掃描相關資訊。

- **被阻止的內送連接數**。
  有人試圖連接您的電腦但被阻止，可能是因為您沒有安裝必要的軟體。此類連接基本上沒有惡意，很可能就是合法的伺服器請求。
- **被阻止的外寄連接數**。
  被一個或多個規則阻止的外寄連接的數量。如果許多外寄連接被阻止，您應該檢查相關規則是否正確。

- **被阻止的連接埠掃描數**。
  顯示有多少系統的嘗試企圖掃描開放連接埠。有時病毒會掃描開放連接埠，試圖進行傳播，但也可能是管理性軟體執行的一次合法操作。

禁用 Personal Firewall (啟用)

按一下連結可在啟用和禁用 Personal Firewall 之間切換。您可以從應用程式的主頁面或系統托盤功能表中，啟用或禁用 Personal Firewall。

- 移至 Personal Firewall 的主頁面，並選擇**禁用 Personal Firewall**。



注釋：Windows 的「資訊安全中心」在防火牆禁用時會發出警告。

或

- 在系統托盤圖示上按一下滑鼠右鍵，並選擇**禁用 Personal Firewall**。





注釋：Windows Vista 沒有這個選項，因此您必須使用控制台禁用和啟用 Personal Firewall。

鎖定

按一下連結可在鎖定和解鎖對網路的所有存取 (包含 Internet) 之間切換。如果在電腦處於開啟狀態時離開，您可能就希望使用此功能。

清除會話規則

選擇此選項可刪除上次重新啟動電腦後建立的暫時防火牆規則。暫時防火牆規則建立於會話期間，即兩次電腦重新啟動之間，您從防火牆彈出對話方塊中選擇**套用於該會話**時。當動作需要您決定是允許還是拒絕時，會彈出此對話方塊。動作是，例如當程式嘗試連線至 Internet 時的動作。系統將提示您確認對規則的移除。

清除阻止規則

如果您無法連線到 Internet/網路，可能是因為某個規則阻止連線。按一下此選項可移除所有阻止規則。系統會在您下次嘗試訪問 Internet 時提示您。

專家工具

請參閱下一節。

專家工具

專家工具包括「規則編輯器」、「即時日誌公用程式」、「進階連接埠查看器」及「匯出與匯入 Personal Firewall 規則」功能。您可以使用這些工具，管理該應用程式的進階層面。

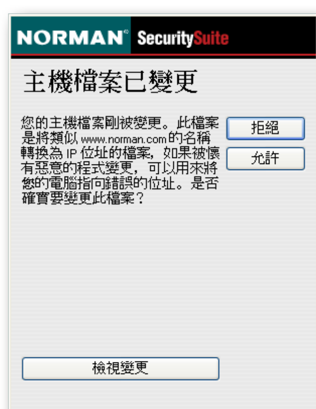
專家工具是為專家級使用者設計的。不過，精靈模式中的「規則編輯器」除外，這項工具非常適合沒有經驗的使用者使用。您可以在「規則編輯器」對話方塊中，在精靈模式和進階模式之間切換。

您可以使用規則編輯器編輯或建立規則。需要使用防火牆規則來允許信任的應用程式訪問 Internet，以及阻止不可靠的連線。防火牆也會使用進階暗中控制技術，讓電腦不可見，也無法從 Internet 偵測到。您可以使用即時日誌公用程式與進階連接埠查看器監視電腦活動。



規則編輯器

要允許「信任的」應用程式訪問 Internet，規則是必需的，如同目前的許多程式所要求的那樣。防火牆已為您在執行安裝精靈時安裝在電腦中的信任程式建立了規則。但是，您可能安裝了防火牆無法辨識的程式，或是在安裝防火牆之後取得的程式。這類程式在嘗試連線到網路時，Personal Firewall 會彈出快顯訊息以告知連線動作，並讓您決定要允許或拒絕動作。



Personal Firewall 不允許您建立內送規則。內送規則是由 Personal Firewall 的「伺服器模式」知覺所處理，它會動態且自動根據「伺服器特權」建立內送規則。這是防火牆中一個很聰明的機制，它會評估從外部偵聽一組連接埠的嘗試。只允許存取相關連接埠的合法請求，當不再需要這些連接埠時，它們會自動關閉。

執行「Personal Firewall 安裝精靈」時，您已在沒有經驗的使用者與有經驗的使用者之間進行了選擇。「規則編輯器」視所選使用者級別而有所不同。

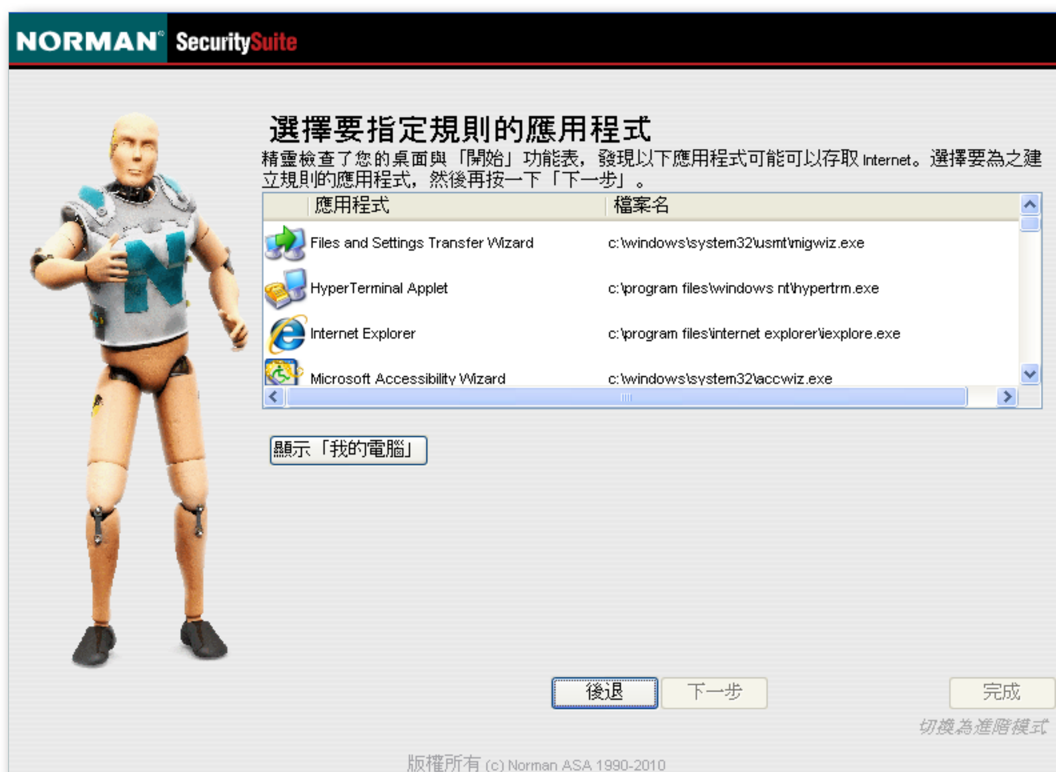
提示

切換使用者模式：在「規則編輯器」對話方塊的右下角有一個用於選擇使用者模式的選項。此選項可在*切換為精靈模式*與*切換為進階模式*之間切換。

沒有經驗的層級（精靈模式）

移至 **Personal Firewall > 專家工具**，並按一下**規則編輯器**來開啟「規則精靈」對話方塊。

1. **規則精靈**
   - 選擇**我想新建一個規則**，再按一下**下一步**。



2. **選擇要指定規則的應用程式。**
   - 顯示合格應用程式的列表。按一下應用程式，來進行選擇。選擇**顯示「我的電腦」**，在電腦中瀏覽列表中沒有的程式。按一下**下一步**繼續。
3. **該應用程式的動作？**
   - 選擇**允許**或**拒絕**此應用程式訪問 Internet。按一下**下一步**繼續。
4. **這是伺服器應用程式嗎？**
   - 決定這是否為伺服器應用程式。伺服器應用程式可以讓連接埠開放並可見，使電腦模擬伺服器的行為方式，允許其他電腦連接到您的電腦。如果不確定，請選擇**否**。按一下**下一步**繼續。

提示

如果應用程式請求伺服器特權，防火牆稍後將提示您。稍後您可以隨時變更規則。

5. **摘要**
   - 隨即顯示摘要對話方塊。按一下**完成**產生規則。
   - 規則產生後會立即生效。

有經驗的層級（進階模式）

移至 **Personal Firewall > 專家工具**，然後按一下**規則編輯器**。隨即顯示一個對話方塊，列出現用規則及其狀態。



1. 按一下**新建**，然後完成必填欄位。
2. 按一下**確定**進行確認。

如需所有欄位的詳細說明，請參閱應用程式說明檔。

即時日誌公用程式

Personal Firewall 會使用進階暗中控制技術，讓您的電腦不可見，也無法從 Internet 偵測到。您可以使用另外兩個功能來監控您電腦上的活動：**即時日誌公用程式**和**進階連接埠查看器**。

移至 **Personal Firewall > 專家工具**，然後按一下**即時日誌公用程式**。在項目上按一下滑鼠右鍵以檢視詳細資訊，並視需要變更此應用程式的配置。



外寄流量

日誌指定**應用程式**聯絡 Internet 的**時間**、程式名稱以及來自哪個**連接埠**，指明**遠端**電腦的 IP 位址、連接埠與**動作**。**動作**可以是「允許」或「拒絕」。**理由**在於存在針對此動作/應用程式的永久規則或會話規則 (假定在**進階配置**或使用者提示超時中定義了的話)。

伺服器特權請求

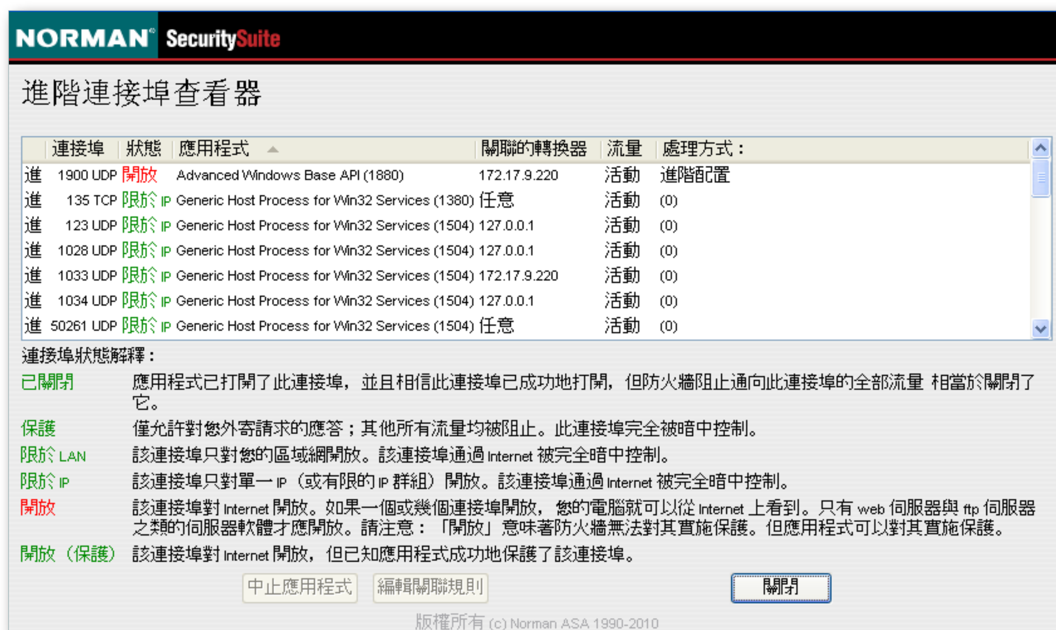
日誌指定**應用程式**在什麼**時間**從 Internet 透過哪個**連接埠**聯絡了您的電腦，指明**遠端**電腦的 IP 位址、連接埠以及 Personal Firewall 採取的**動作**。**動作**可以是「允許」或「拒絕」。**理由**在於存在針對此動作/應用程式的永久規則或會話規則，這是在**進階配置**中定義的，或者沒有偵聽應用程式。不允許伺服器特權請求的最常見理由在於使用的電腦沒有必需的軟體來解釋詢問。換而言之，就是不匹配伺服器特權請求。

若要從網路中的其他電腦接收資料，應用程式將打開一個或多個偵聽連接埠。請注意：伺服器特權請求並非是已建立的連接，而是連接請求。但有時應用程式也會打開一個偵聽連接埠，以便從給它傳送資料的電腦接收應答。Personal Firewall 將自動允許這類應答。Personal Firewall 的其中一種機制將確定應用程式是否已有意開啟了連接埠，或者應用程式是否被視為伺服器而接收了一個主動提供的請求。Personal Firewall 隨後提示使用者確認應將應用程式視作伺服器而授予特權。

進階連接埠查看器

「進階連接埠查看器」概述目前電腦連接埠上的所有活動。您應該使用此公用程式，手動檢查您的電腦以確定沒有遭到惡意軟體感染。

移至 **Personal Firewall > 專家工具 > 進階連接埠查看器**。



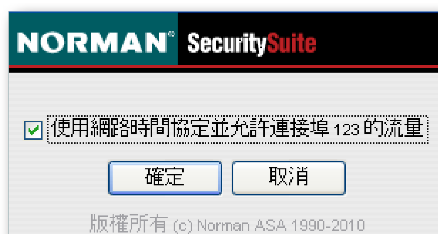
對 Internet 開放的連接埠會以紅色顯示，且應該獲得您的高度注意，因為防火牆無法保護開放連接埠。FTP 和 Web 伺服器等伺服器軟體可以合法使用開放連接埠。但是如果未知的應用程式在開放連接埠上處於活動狀態，就有理由要擔心。

停止應用程式

若要停止應用程式，請將項目反白，並按一下**中止應用程式**。應用程式會立即中止，雖然之後它可能會列表中顯示大約一分鐘。

進入「打開進階配置」

反白項目，並選擇**打開進階配置**選項。





注釋：若要將應用程式的配置從允許變更為拒絕，請清除核取方塊，並按一下確定。或者，選擇核取方塊以允許被拒絕的應用程式訪問 Internet。請注意，「中止應用程式」和「編輯關聯規則」只會套用到「由規則處理」的項目。「打開進階配置」選項只供由「進階配置」處理的規則使用。

匯出 Personal Firewall 規則

備份您的 Personal Firewall 規則。選擇**匯出 Personal Firewall** 規則，並指定位置。將檔案儲存至外部媒體以妥善保管。

匯入 Personal Firewall 規則

復原您的 Personal Firewall 規則。選擇**匯入 Personal Firewall** 規則，並指定要從哪個位置復原備份檔案。

設定

配置 Personal Firewall

在設定期間，系統自動建立了幾個規則，包括適合於大多數瀏覽器的規則、電子郵件用戶端規則、MSN 以及需要連接網路的其他程式的規則。

移至 **Personal Firewall > 設定 > 配置 Personal Firewall**。若要檢視及/或編輯現用規則，請參閱第 33 頁的「規則編輯器」。

外寄應用程式

某些未指定規則的應用程式可能會嘗試連線到 Internet 或區域網。您可在此對話方塊中，決定 Personal Firewall 應如何處理這些應用程式。預設設定為**提示**。例如，您可以在系統提示時，評估嘗試連線的應用程式並定義規則。另一種選擇是**拒絕**，在這種情形下，沒有永久性規則或者基於會話規則的所有程式都將被拒絕訪問網路。

伺服器特權

某些未指定規則的應用程式可能會嘗試接受來自 Internet 的連線。您可在此對話方塊中，決定 Personal Firewall 應如何處理這些應用程式。預設設定為**提示**。您可以在系統提示時，評估應用程式是否應接受來自網路的邀請。另一種選擇是**拒絕**，在這種情形下，沒有永久性規則或者基於會話規則的所有程式都將拒絕來自網路的邀請。



注釋：「編輯規則」對話中有一個選項，允許您給應用程式授予伺服器特權或者拒絕此特權。伺服器特權這一概念還將在編輯規則**主題中解釋。**

進階設定

這些配置選項的技術特性決定了如果您打算變更預設設定，您就需要具備一定的專門技術。除非您真正瞭解設定，並清楚變更後的後果，否則，請不要變更任何設定，這是經驗之談。預設設定對於一般使用者已經足夠。

「防火牆執行」選項如下所述。如需所有選項的詳細資訊，請參閱應用程式說明檔。

切換使用者模式（沒有經驗/有經驗）

移至 **Personal Firewall > 設定 > 進階設定**，然後向下捲動至**防火牆執行**部分。

防火牆執行

☑ 使用進階規則編輯器

如果您在設定期間指定了「有經驗的使用者」，則該選項就啟用。如果您在設定期間指定了「沒有經驗的使用者」，您就應該啟動規則精靈。這兩個使用者層級的不同在於您在建立新規則或變更現用規則時所獲得的協助程度。如需有關如何在兩種不同模式中建立規則的詳細資訊，請參閱第 33 頁的「規則編輯器」。

Antispam

開啟 Security Suite 應用程式，並從左側功能表中選擇 **Antispam**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」，關於應用程式的目的與功能說明，請參閱第 7 頁的「Antispam」。

主頁面



此應用程式可為您阻止不必要的，且可能包含系統威脅之商務與大量電子郵件（垃圾郵件）。本章介紹如何自訂垃圾郵件篩選器、建立阻止和允許列表、管理篩選的電子郵件、檢視篩選的電子郵件，以及如何設定更新間隔與垃圾郵件管理選項。

垃圾郵件統計資訊

圖形視圖顯示，在過去兩週之中，應用程式每天擷取的垃圾郵件數量，與阻止的網路釣魚嘗試次數。

自訂設定

按一下此選項可編輯預設值。請參閱第 43 頁的 Antispam「設定」。關於選擇建議及自訂設定的一般資訊，請參閱第 15 頁的「Security Suite 設定」。

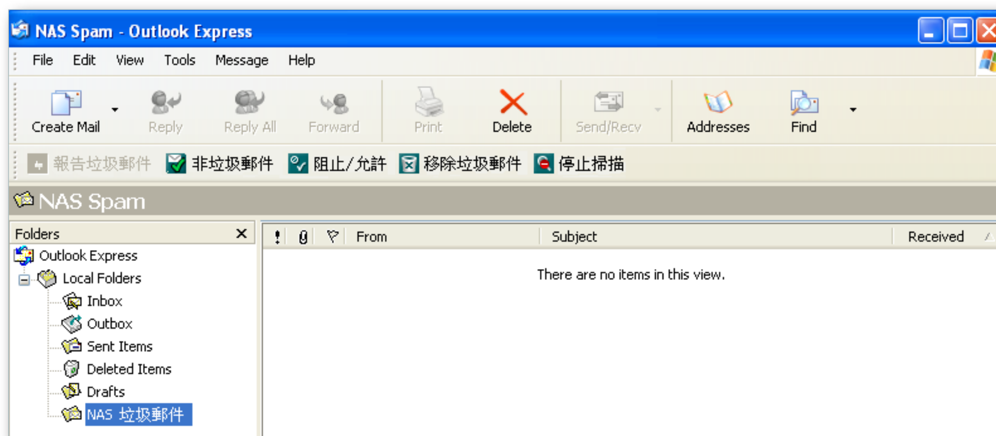
阻止/允許

您可以使用「阻止/允許」列表管理個人電子郵件地址，以通知應用程式應始終允許或拒絕的地址。防垃圾郵件篩選方法絕不會使您手動指定的地址失效（「阻止」或「允許」）。請參閱第 42 頁的「阻止/允許」。

檢視篩選的電子郵件

您可以從電子郵件應用程式中 (例如 Microsoft Outlook、Outlook Express 或 Windows Mail)，檢視篩選為垃圾郵件的電子郵件。當您安裝 Norman Security Suite，或在電腦上已安裝 Norman Security Suite 的情況下，安裝上述其中一個電子郵件用戶端時，會建立「NAS 垃圾郵件」資料夾。

開啟您自己喜好的電子郵件用戶端，然後找到「NAS 垃圾郵件」資料夾與 Antispam 應用程式功能表。



- **報告垃圾郵件**
  - 將電子郵件報告為垃圾郵件。從「收件匣」中選擇電子郵件，然後從工具列中按一下**報告垃圾郵件**。會將郵件移到 **NAS 垃圾郵件**資料夾。
- **非垃圾郵件**
  - 將電子郵件標示為非垃圾郵件。從 **NAS 垃圾郵件**資料夾中選擇一或多封電子郵件，並按一下**非垃圾郵件**。
- **阻止/允許**
  - 阻止或允許電子郵件。選擇此選項，開啟 Norman Antispam 應用程式。輸入要**阻止**或**允許**的一或多個電子郵件地址。
- **移除垃圾郵件**
  - 清除 **NAS 垃圾郵件**資料夾的全部內容。若要一次刪除一封郵件，請在項目上按一下滑鼠右鍵，然後從快顯功能表中選擇**刪除**。
- **掃描資料夾**
  - 掃描內送電子郵件是否為垃圾郵件。選擇一或多個資料夾，然後按一下「掃描資料夾」來啟動手動掃描。此選項可在**掃描資料夾**與**停止掃描**之間切換。按一下**停止掃描**來停止掃描垃圾郵件。

請參閱第 43 頁的「垃圾郵件管理」來指定您是否要自動刪除垃圾郵件。

阻止/允許

您可以手動輸入要阻止或允許的電子郵件地址。選擇輸入欄位旁邊的相關選項按鈕，以指定阻止或允許電子郵件地址。

Antispam > 阻止/允許　說明

阻止或允許電子郵件地址

允許　阻止　新增

範例:name@domain.com、domain.com

電子郵件地址	允許	阻止
沒有供顯示的專案。		

移除所選專案　儲存

新增/移除電子郵件地址

電子郵件地址將出現在對話方塊底部的列表中。當您輸入新地址時，預設選項是**阻止**，這可避免不慎允許要阻止的地址。或者，選擇**允許**以接受來自此寄件者的電子郵件。您可以隨時在電子郵件地址列表中編輯詳細資訊。

新增

1. 輸入電子郵件地址，例如
   `name1@domain.com`
   或
   - 輸入幾個以逗號分隔的電子郵件地址，例如
     `name1@domain.com, name2@domain.com`

   或
   - 輸入要允許或阻止的完整網域，例如
     `phoneysales.com`
   - 注釋：請勿新增您自己的網域，以避免詐騙電子郵件。
2. 針對每個地址，選擇**允許**或**阻止**（預設選項）。
3. 針對每個新項目，按一下**新增**。
4. 按一下**儲存**以保留新的地址或網域。

移除

1. 選擇一個或多個地址。
2. 按一下**移除所選專案**。
3. 按一下**儲存**確認變更。

編輯

1. 選擇一個或多個地址。
2. 根據需要對要阻止/允許的電子郵件地址進行變更。
3. 按一下**儲存**確認變更。

設定

就如同防毒應用程式運用病毒定義檔偵測惡意軟體一般，Antispam 解決方案使用定義檔篩選不必要的電子郵件。病毒定義檔含有決定檔案是否受感染的病毒特徵，而 Antispam 定義則使用一組條件判斷電子郵件是垃圾郵件的可能性。垃圾郵件定義是根據郵件所含的語言、圖片、色彩、連結以及寄件者的電子郵件與 IP 地址進行電子郵件分析。不過，這仍無法完全確定電子郵件是否為垃圾郵件。



配置篩選器嚴格程度

如果您使用滑桿將嚴格程度設定為**低**，Antispam 應用程式將僅檢查最「可疑」的電子郵件，因此會有較少的電子郵件被標示為垃圾郵件。同樣地，如果將滑桿設定為**高**，則會以嚴格的垃圾郵件標準進行檢查，而使得分數不高的電子郵件即被標示為垃圾郵件。

如果幾乎確定或完全確定郵件就是垃圾郵件，例如寄件者出現在黑名單或線上資料庫中，則不論滑桿的位置為何，一律都會阻止該郵件。我們認為預設設定**中**適合用來篩選不必要的電子郵件。

防垃圾郵件篩選方法絕不會使您手動指定的地址失效。

配置垃圾郵件控制

更新垃圾郵件定義

選擇垃圾郵件定義檔更新的頻率；每 5 分鐘、每天一次或每週一次。建議的設定為**每 5 分鐘**。

垃圾郵件管理

此選項可讓您選擇何時刪除已被垃圾郵件篩選器阻止的電子郵件（根據存留期或數量）。預設設定為**下列時間後即刪除全部垃圾郵件**：[10] **天**，並且**超過以下總計即刪除垃圾郵件**：[500] 篩選出的電子郵件。

別忘了按一下**儲存**，確認所有變更。

Parental Control

開啟 Security Suite 應用程式，並從左側功能表中選擇 **Parental Control**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」；關於應用程式的目的與功能說明，請參閱第 7 頁的「Parental Control」。

首次存取

首次使用該應用程式之前，資訊訊息「*未建立管理員！*」會顯示在「首頁」對話方塊中，且黃色的警告三角形會顯示在應用程式的功能表項目上。



1. **未建立管理員**

第一次存取 Parental Control 時，您必須先建立管理員使用者。輸入密碼，並選擇預設的回退配置檔案。按一下**儲存**繼續。

預設的回退配置檔案應該是您要建立的最低等級使用者配置檔案。也就是說，如果您要建立「兒童」配置檔案，則預設的回退配置檔案也應該是「兒童」。只有管理員能夠編輯使用者和配置使用者的設定 (例如排定 Internet 訪問的時間)，並且建立阻止和允許列表。管理員一般都是父母。

稍後您可以從 **Parental Control > 設定**中變更這些設定。



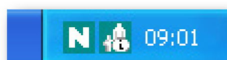
注釋：無法重設管理員密碼。務必選擇您容易記住的密碼。密碼區分大小寫。

2. **管理員登入**

當管理員使用者已建立時，登入頁面便會出現。使用管理員的使用者名稱與密碼登入以存取應用程式。

系統托盤圖示

系統托盤圖示表示已安裝 Parental Control。將滑鼠游標移到圖示上，會顯示狀態文字，例如「Parental Control：「管理員」已登入」。



主頁面



此應用程式能夠阻止對某些類別的網站進行訪問，它還會為使用者限制及排程 Internet 訪問。本章介紹如何建立、配置與管理使用者，以及如何檢視日誌與排程 Internet 訪問。使用管理員的使用者名稱與密碼登入以存取應用程式。

設定

按一下此選項可編輯預設值。請參閱第 50 頁的 Parental Control「設定」。

統計資訊

您可以在主頁面中，追蹤已阻止和已掃描元素的統計資訊。

使用者配置

請參閱第 46 頁的「使用者配置」。

日誌查看器

請參閱第 50 頁的「日誌查看器」。

使用者配置

建立使用者並指定使用者配置檔案。現有使用者會列在此對話方塊中，其中會顯示使用者名稱，以及已指定給該使用者的配置檔案。



有三種使用者配置檔案，分別是**成人**、**青少年**與**兒童**。後者完全受限，並且僅可訪問管理員在允許列表中手動輸入的網址。

成人	沒有任何限制。
青少年	類別篩選器限制。
兒童	完全限制。

類別

類別採用各種術語與措辭供 Parental Control 識別網頁，例如識別主要以性為主的網頁。這些術語不可檢視或進行編輯。對於「青少年」配置檔案而言，共有四大類別可用於阻止訪問**性**、**賭博**、**武器**和**毒品**內容的網頁。預設情形下所有類別均開啟，但管理員可以取消應該准許的類別。

阻止/允許列表

對於「兒童」配置檔案的使用者而言，必須要有允許列表，因為該群組的使用者只能檢視此列表上的網址。對於「青少年」配置檔案的使用者而言，可以選擇是否建立阻止列表和允許列表。請參閱第 47 頁的「預設「兒童」配置檔案」和第 47 頁的「預設「青少年」配置檔案」。

網址格式

URL (統一資源定位器) 是網址的技術性稱呼。網址中不支援通配符 (*/?)。有效的格式有：

- http://www.newspaper.com
- www.newspaper.com
- newspaper.com

指定的網址可讓您造訪子網域層級，但不可造訪父層級。例如，允許訪問 www.newspaper.com/kidsstuff 並不一定會允許訪問其父層級 www.newspaper.com。但是，如果新增 newspaper.com，則允許訪問該網址的所有子網域層級，如 news.newspaper.com、cartoon.newspaper.com 等。



注釋：如果使用者追隨允許的網頁上的連結，這就屬於允許之列，無論該連結最終引向何處。但是，除非引用網頁被明確允許，否則，就不能開啟其他網頁。

預設配置檔案設定

成人配置檔案沒有限制。**兒童**和**青少年**配置檔案受到限制，因此可以配置。事實上，如果指派給**兒童**配置檔案的使用者真的要訪問 Internet，則必須指定網頁。這些配置檔案設定適用於使用者配置檔案的所有成員。若要配置個別成員，請參閱第 48 頁的「建立使用者」。

預設「兒童」配置檔案

請注意，您對此預設配置檔案所做的變更將影響配置檔案的所有成員，並不侷限於個別的使用者。除了明確允許的網頁外，「兒童」配置檔案的所有網頁都會受到阻止，所以此配置檔案使用者不具有阻止列表或類別。

新增

1. 在**將地址新增至列表**欄位中輸入要允許的網址。
   - 若要輸入多個網址，請用逗號分隔。
2. 針對每個新項目按一下**新增**。

移除

1. 選擇一個或多個地址。
2. 按一下**移除所選專案**。

預設「青少年」配置檔案

請注意，您對此預設配置檔案所做的變更將影響配置檔案的所有成員，並不侷限於個別的使用者。「青少年」配置檔案依據「類別」和「阻止/允許」列表限制網頁。

Parental Control > 使用者配置　說明

預設「青少年」配置檔案

注意! 這些配置檔案設定適用於使用者配置檔案的所有成員。

類別 | 阻止/允許列表

「青少年」配置檔案根據類別中的設定阻止網頁。您可以新增一個或多個網頁，以允許存取先前阻止的網頁。

將地址新增至列表

允許　阻止　新增

範例：http://www.newspaper.com;www.fun.com;www.totlers.com

	地址	允許	阻止
☐	friendsgroup.org	◉	○
☐	www.favoritedomain.com	◉	○

移除所選專案　儲存

類別

預設情形下會選取所有類別，即「青少年」配置檔案會根據這些設定阻止具有某些內容的網頁。這些類別包括「性」、「賭博」、「武器」和「毒品」。管理員可以移除勾號，允許該類別的網頁。另外，也可以新增一個或多個網頁至「允許」列表。按一下**儲存**確認任何變更。

阻止/允許列表
「青少年」配置檔案根據「類別」中的設定阻止網頁。您可以新增一個或多個網頁，以允許訪問先前阻止的網頁。

新增

1. 在**將地址新增至列表**欄位中輸入要允許的網址。
   - 若要輸入多個網址，請用逗號分隔。
2. 針對每個新項目按一下**新增**。
3. 選擇**阻止**或**允許**選項按鈕。
4. 針對每個新項目按一下**新增**。

建立使用者

從 **Parental Control > 使用者配置**中選擇**建立使用者**。

1. 輸入新使用者的名稱，然後輸入您必須確認的密碼。
2. **選擇**新使用者所依據的**預設配置檔案。**
   - 將配置檔案指定給使用者時，您就決定了使用者可以檢視哪類網頁：
     - 成人
       沒有任何限制。使用者可以訪問任意網站。
     - 青少年
       大體上沒有任何限制。但是，預設類別設定會阻止包含不宜主旨或內容的網頁。
     - 兒童
       只允許檢視管理員在「允許列表」中輸入的網頁。
3. 按一下**儲存**進行確認。
   - 按一下**儲存**以建立新的使用者之前，您應該檢查是否針對指名的使用者選擇正確的配置檔案。

會將新使用者新增至使用者列表。按一下使用者名稱即可配置該使用者。

變更密碼
變更所選使用者的名稱和密碼。

類別
本選項僅適用於「青少年」配置檔案使用者。若要允許「青少年」配置檔案使用者的一個或多個類別，請清除相關類別核取方塊。如需詳細資訊，請參閱第 46 頁的「類別」一節及第 47 頁的「預設「青少年」配置檔案」。

阻止/允許列表
本選項僅適用於「青少年」配置檔案使用者。您可以在這裡允許或阻止使用者訪問的網址。如需詳細資訊，請參閱第 46 頁的「阻止/允許列表」及第 47 頁的「預設「青少年」配置檔案」各節。

允許列表
本選項僅適用於「兒童」配置檔案使用者。您可以在這裡允許使用者訪問的網址。請亦參閱第 47 頁的「預設「兒童」配置檔案」。

排程器
管理員可以確定使用者在每週的哪些時間段可以訪問 Internet。預預設設定是允許所有時段 (綠色)。

Parental Control > 使用者配置 說明

Child 配置檔案: User1

變更密碼 允許列表 排程器

計劃 Internet 存取時間。按一下適當的方塊以選取日期/時間。按住並拖曳游標可指定需要的時段。

Allow Deny

	星期一	星期二	星期三	星期四	星期五	星期六	星期天
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							

1. 若要在一段特定的時間內阻止 Internet 訪問，請將游標放在所需的時段中，並按一下該時段。
2. 在按住游標的同時，往上、下、左、右拖曳游標，以擴大您想要拒絕的時段。以同樣的方式按住並拖曳游標，可從**拒絕**（灰色）變更為**允許**（綠色）。
3. 按一下**儲存**確認變更。

日誌查看器

Parental Control 會自動記錄為「青少年」與「兒童」配置檔案使用者阻止的網頁。但日誌並不顯示使用者具體訪問了哪些網頁。

日誌可以顯示最多一週前禁止的網頁。一週的每天都有一個日誌，您只能選擇工作日，不能選擇日期。Parental Control 建議將目前工作日用作預設設定。

日誌的各欄分別顯示日期、時間、使用者名稱、被禁止的原因以及被禁止的 URL。

如果「使用者」欄留空，表明系統已經進入回退模式，沒有使用者登入。

設定

可以避免以成人身份登入的電腦在無人看守的情形下被兒童使用 （亦即，如果忘記登出或需要突然離開電腦時)。預設回退配置檔案將在指定空閒時間之後啟動。

變更預設配置檔案之前的空閒時間

空閒時間是系統沒有活動的時間，也就是沒有按下鍵盤，也沒有移動滑鼠。

- 從下拉功能表中，選擇電腦閒置後 Parental Control 應該何時採用預設配置檔案。
- 按一下**儲存**進行確認。

設定預設回退配置檔案

您可以選擇「青少年」或「兒童」，做為 Parental Control 在過了指定的空閒時間後應採用的配置檔案。

- **兒童**
  「兒童」配置檔案阻止所有的網頁，但不包括您手動輸入的網頁。這表示在您為「兒童」使用者新增網頁之前，將無法訪問 Internet。
- **青少年**
  根據類別中的設定 (也就是性、賭博、武器和毒品)，「青少年」配置檔案阻止包含某些內容的網頁。
- 按一下**儲存**進行確認。

變更管理員密碼

管理員密碼無法重設，但如果您知道舊密碼，則可變更密碼。如果變更了管理員密碼，您最好將其寫下來，放到安全的地方。



注釋：請注意密碼區分大小寫

Privacy Tools

開啟 Security Suite 應用程式並從左側功能表中選擇 **Privacy Tools**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」；關於應用程式的目的與功能說明，請參閱第 7 頁的「Privacy Tools」。



您可以使用該應用程式執行特定檔案的安全刪除。檔案的內容會永久清除且無法復原。您也可以配置應用程式，使其自動刪除包含個人資料、cookie 和瀏覽器記錄的各種日誌檔案。刪除記錄日誌並不會影響應用程式的設定與書籤。

刪除使用者的程式記錄

使用者名稱列表顯示此電腦的所有已註冊使用者，程式列表顯示可以選擇從中刪除記錄日誌的應用程式。

- 選擇要刪除記錄的一個或多個使用者名稱和程式。
- 按一下**立即刪除記錄**進行確認。

手動或自動刪除記錄

您可以手動刪除記錄日誌，也可以配置應用程式以指定時間間隔自動刪除。

- **手動**。
  記錄日誌只會在您按一下**立即刪除記錄**時刪除。
- **每 10 分鐘**或**每小時**。
  記錄日誌將依選取頻率自動刪除。
- 按一下**儲存**進行確認。



注釋：如果您選擇手動**刪除記錄，只有在您按一下**立即刪除記錄**時才會清除日誌。記錄日誌「不」會自動被刪除。**

安全刪除

您可以使用該應用程式執行特定檔案的安全刪除。檔案的內容會永久清除且無法復原。

您只要按一下滑鼠右鍵，就可以啟動檔案的安全刪除程序。系統將提示您確認刪除。刪除進度將會顯示，且會在刪除程序完成時顯示摘要。安全地刪除檔案的方法如下：

- 選擇一個或多個要刪除的檔案。
- 在檔案上按一下滑鼠右鍵。
- 從快顯功能表中選擇 **Norman Secure Delete**。
- 按一下**確定**進行確認。
- 按一下**確定**，關閉摘要對話方塊。

檔案內容在已從您的電腦中永久清除。



注釋：使用安全刪除方法刪除檔案，遠比普通的檔案刪除更為耗時。這是因為會多次覆寫檔案的每個部分，以防止原始內容的任何記錄被復原。

如果您在刪除程序啟動後將其停止，則檔案仍會銷毀，但不會如預期般安全。

某些檔案可能不會被刪除。這可能是因為使用者沒有檔案的寫入權限，或檔案受到作業系統的保護，無法刪除。

Intrusion Guard

開啟 Security Suite 應用程式並從左側功能表中選擇 **Intrusion Guard**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」；關於應用程式的目的與功能說明，請參閱第 8 頁的「Intrusion Guard」。

主頁面



該應用程式是專為有經驗的使用者設計的主機型入侵防範系統 (HIPS)。沒有經驗的使用者應使產品配置保持為建議的設定，這在多數情況下是允許並記錄事件。預設情況下，只會阻止具有高度風險且很少由合法應用程式使用的事件。

自訂設定

按一下此選項可編輯預設值。請參閱第 53 頁的「設定」。關於選擇建議及自訂設定的一般資訊，請參閱第 15 頁的「Security Suite 設定」。我們建議只讓進階使用者自訂這些設定 (即預設設定)。

進階系統報告器

這是專為有經驗的使用者設計的工具。它具有可讓您透過搜尋電腦上的異常情況，偵測未知間諜軟體和 rootkit 的功能。請參閱第 64 頁的「附錄 B」。

設定

您可在此對話方塊中檢視和編輯應用程式的配置。在此對話方塊最頂端的部分，選擇**自訂設定**以變更預設設定，或選擇**建議的設定**以切換回預設配置。



注釋：我們建議只讓進階使用者變更預設設定。

驅動程式與記憶體

Intrusion Guard > 設定 說明

目前設定: **建議** 自訂設定

驅動程式與記憶體 | 程序 | 網路

驅動程式安裝

系統驅動程式可以存取及控制硬體裝置，為執行此操作，它被授予了完整的系統存取權，甚至超出以管理員權限執行的應用程式的存取權。如果應用程式嘗試在您的系統上安裝驅動程式，Intrusion Guard 應該怎麼辦？

提示 允許 拒絕

實體記憶體存取 (僅限 32 位元)

透過直接操縱實體記憶體，應用程式可執行通常受到作業系統保護的工作。如果應用程式嘗試存取實體記憶體，Intrusion Guard 應該怎麼辦？

提示 允許 拒絕

載入及執行驅動程式 (僅限 32 位元)

惡意應用程式會嘗試載入系統驅動程式，而不先安裝它。當應用程式嘗試執行直接載入並執行驅動程式的作業時，Intrusion Guard 應該怎麼辦？

提示 允許 拒絕

儲存

驅動程式是在低層級運作的電腦程式，此層級通常稱為「核心層級」。驅動程式的設計目的通常是為了存取及控制硬體，例如顯示監視器、鍵盤、印表機和網路卡。為了存取連接電腦的硬體，驅動程式需要有完整的系統存取權。因此，編寫惡意應用程式時也會使用相同的技術。您可以修改驅動程式安裝配置，以控制允許哪些應用程式在您的電腦上安裝驅動程式。

有兩種惡意技術可獲取與驅動程式相同的權限。這兩種技術都會規避作業系統的安全機制。高度建議您將這兩者的設定都保持為**拒絕**。

- **提示**
  每次發生該嘗試時都會詢問您。
- **允許**
  只會記錄這些嘗試。
- **拒絕**
  無論合法或惡意應用程式都無法安裝核心層級驅動程式。

程序

Intrusion Guard > 設定 說明

目前設定: **建議** 自訂設定

驅動程式與記憶體 | **程序** | 網路

自動啟動保護

應用程式可以指示作業系統在每次電腦啟動時或使用者登入時自動啟動該應用程式。當應用程式嘗試執行此工作時，Intrusion Guard 應該怎麼辦？(請注意，此功能並不包含 CD 或 USB 隨身碟的自動執行功能。)

提示 允許 拒絕

服務安裝

應用程式可以將自身安裝成背景服務，這會使它在每次電腦啟動時執行，並以系統權限執行。當應用程式嘗試安裝服務時，Intrusion Guard 應該怎麼辦？

提示 允許 拒絕

程序保護 (僅限 32 位元)

當應用程式嘗試將執行緒或其他程式碼插入到其他程序中以劫持該程序時，Intrusion Guard 應該怎麼辦？

允許 拒絕

儲存

如果您的電腦上安裝了合法或惡意應用程式，該程式通常會想要在每次啟動您的電腦時自動啟動。想要自動啟動的程式可以指示作業系統使用與目前使用者相同的權限自動啟動其本身，或者也可安裝以升級權限執行的背景服務。此入侵防範應用程式可將這兩類嘗試都停止。

- **提示**
  每次發生該嘗試時都會詢問您。
- **拒絕**
  無論合法或惡意應用程式，都無法將其本身安裝為在電腦啟動時自動啟動。

程式也可將程式碼插入在您電腦上執行的其他程序，或是透過其他方式劫持程序。這是惡意應用程式的常見行為，但某些合法程式也會使用此類技術，例如，用於擴展使用者的桌面，或提供其他進階功能給作業系統或協力廠商應用程式。您可以配置應用程式，使其對每個這類嘗試加以拒絕或提示。

您可以編輯受信任的應用程式列表，使其包含通常會嘗試此類行為的合法應用程式。

網路



惡意應用程式可新增篩選器至作業系統中的網路模組，以竊取個人資料 (例如身份證號碼、信用卡詳細資訊和密碼)。廣告軟體可修改透過這些篩選器傳送的網路資料。它可以變更搜尋引擎中的結果，並在您桌面上顯示及在所造訪網頁中內嵌不需要的廣告。

BHO (瀏覽器幫助對象) 是 Microsoft Internet Explorer 的擴展。這個外掛程式以及其他 Internet Explorer 外掛程式 (例如工具列) 對進出 Internet Explorer 的網路流量有完整的控制權，而且能與使用者介面互動。

LSP (層次服務提供者) 是 Windows 中網路堆疊內的一般性篩選器。它對您電腦上的所有網路流量有完整的控制權。

當您透過網站的網域名稱 (網址) 訪問網站時，會將網域名稱轉換為 IP 位址。然後會將資料傳送至遠端伺服器及從遠端伺服器傳送資料。您的電腦會先在您的主機檔案中尋找網域名稱。這表示該處的項目將覆寫名稱將解析為的任何 IP 位址。惡意應用程式可變更您的主機檔案，從而將網路流量重定向至惡意網站 (即所謂的「Pharming」)。

- **提示**
  每次發生事件時都會詢問您。
- **拒絕**
  所有修改您的系統和主機檔案、安裝 BHO 和 LSP 的嘗試都會遭到阻止。

安裝和更新

開啟 Security Suite 應用程式並從左側功能表中選擇**安裝和更新**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」。

主頁面



除了其他選項，**安裝和更新**功能表會顯示 Security Suite 中所有可用產品的列表。您可以從這個功能表中新增或移除產品、啟動更新、啟動「授權精靈」，及變更 Norman Security Suite 安裝的語言。



注釋：此頁面變更需要系統重新啟動，才會生效。

自訂設定

按一下此選項可編輯預設值。請參閱第 58 頁的「設定」。關於選擇建議及自訂設定的一般資訊，請參閱第 15 頁的「Security Suite 設定」。

授權的產品

授權產品的列表會顯示已安裝哪些產品、它們的狀態，以及授權何時過期。您可以在此頁面中新增或移除列表中的產品或元件。如果清除一個核取方塊，對應的產品就將被徹底卸載。將新產品或元件新增至 Norman Security Suite 時，會自動下載它們。所有選取的產品均可透過 Norman Security Suite 的「Internet 更新」功能自動更新。



注釋：如果清除產品核取方塊，取消的產品就將被卸載並永遠不會更新。

更新全部的產品

我們時常為病毒定義及程式檔案提供更新。更新透過 Internet 或內部網路完成。Internet 更新一旦完成套裝軟體的下載，實際的更新就將自動安裝。更新之後，程式可能會提示您重新啟動電腦。

- 按一下**更新全部的產品**，更新整個 Security Suite。

啟用/禁用自動更新

預設情形下自動更新均開啟。這表示當有元件或定義檔可更新時，會更新產品安裝。若要變更自動更新設定，請參閱**設定 > 選擇更新方式**一節。

注釋：防毒軟體必須時常更新，才能有效發現及移除惡意軟體。

選擇產品語言

您可以變更在安裝時選擇的語言。從**產品語言**下拉功能表中選擇偏好語言，然後按一下**儲存**。變更將於下次更新之後生效。

授權精靈

「授權精靈」會檢查及更新授權。如果您選擇此選項，會出現對話方塊，其中包含有關安裝的產品與許可密鑰憑證的資訊。更新安裝需要有效的密鑰。

設定

選擇更新方式

此選項可讓您選擇手動更新或自動更新。我們建議使用自動更新方法，因為隨時保持軟體的最新狀態至關重要。

手動更新

如果您希望從「安裝和更新」主頁面（更新全部的產品）手動啟動 Internet 更新，請選擇此選項。您也可以從系統托盤功能表選擇「Internet 更新」。



注釋：手動更新選項需要強迫啟動「Internet 更新」功能。選擇此選項表示系統「不會」自動更新。強烈建議您時常更新軟體。對於每日使用來說，不建議使用手動更新方法，因為您可能很容易忘記執行更新。

依據設定間隔自動更新

選擇此選項即可讓程式自動進行下載與更新。從**自動更新間隔**旁的列表中選擇一個時間間隔，設定需要的間隔。此選項需要永久連線至 Internet。



注釋：依據設定間隔自動更新選項表示系統會自動更新。這是建議的更新方法。如果「Internet 更新」未執行達 24 個小時之久，該程式會在啟動時自動檢查是否有更新。

等待撥號連線

如果使用數據機來連線 Internet，請選擇此選項，以便每天從產品伺服器上檢查更新。只要如往常般訪問 Internet，該程式便會知道是否有更新檔案。如果您每日連線到 Internet 數次，更新機制只會在您第一次連線時檢查更新。如果您一週連線一次 Internet，只要您連線，程式就將檢查一次。

Proxy 設定

Proxy 伺服器就是位於使用者電腦與 Internet 之間的一台中間電腦。可以用來記錄 Internet 的使用，並阻止對某個網站的訪問。Proxy 伺服器上的防火牆還可以用來阻止對某些網站或網頁的訪問。

若有防火牆或 Proxy 伺服器保護您的電腦，您必須輸入所需的 Proxy 資訊。

- 移至**安裝和更新 - 設定 - Proxy 設定**。
- 選擇**使用 Proxy 伺服器**並輸入 Proxy 位址與連接埠。
- 如果適用，請選擇**登入 Proxy 伺服器**並輸入使用者名稱、密碼與網域 (針對 Windows NT Challenge/Responses)。
    - Windows Challenge/Response Authentication 是用於連接 Windows 2000 Server 或 Exchange 的格式。
    - 使用者帳號具有如下格式：[*NT/2000 網域名稱*]\[*帳戶名稱*]

支援中心

開啟 Security Suite 應用程式並從左側功能表中選擇**支援中心**。關於開啟應用程式的方法，請參閱第 13 頁的「入門」。

主頁面



支援中心提供何處可以取得更多協助（除了產品文件及線上說明之外）的相關資訊。其中也包含自動修復功能，如果您在使用已安裝的軟體時遇到問題，這可能會有幫助。

說明與疑難排解

按一下**說明與疑難排解**連結可將您帶往 Norman 網站，此網站中有各種很有用的資源，在大多數的情況下對您很有幫助。在此網站上有：

- 支援
- 資訊安全中心
- **Norman 支援論壇**

如果搜尋這些資源無法解決問題，請與您當地的經銷商或 Norman 辦公室聯絡。

聯絡資訊

此頁面上有電話號碼和地址，讓您能夠與當地的 Norman 辦公室/代表聯絡。本文件最後一頁也有此資訊。

自動修復

如果您在使用安裝的 Security Suite 版本時碰到任何問題，請先嘗試執行自動修復，再與支援人員聯絡。

按一下**自動修復**後，系統會在背景啟動檢查您安裝的程式，並視需要更新檔案或元件。在執行自動修復時，您會在系統托盤功能表中看到齒輪符號。如需影響 Security Suite 的圖示解釋，請參閱第 17 頁的「托盤圖示」。

如果您沒有使用圖形使用者介面，您可以執行 `C:\Program Files\Norman\nvc\bin` 中的 `delnvc5.exe`，再選擇**修復**選項。

訊息日誌查看器

這是監視應用程式及顯示各種訊息資訊 (包括類型、始發者、時間和日期、應用程式及詳細資訊) 的功能。

解除安裝 NSS

若要解除安裝 Norman Security Suite，可以使用兩種方法。其一是使用 Windows **新增或移除程式**功能。另一個方法是使用 Norman 的解除安裝應用程式。

1. 從 Windows 作業系統：
   - 選擇**開始 > 控制台 > 新增或移除程式**。
     - 在 Vista 上，您可以選擇**程式和功能**。
   - 請捲動，尋找並選擇 Norman 應用程式。
   - 選擇**移除**選項。
     - 移除程式後，請重新啟動電腦。

2. 使用 Norman 的解除安裝應用程式：
   - 選擇**開始 > 執行**，然後輸入 `delnvc5.exe` 的位置
     - 預設位置為 `C:\Program Files\Norman\nvc\bin\delnvc5.exe`。
   - 選擇**移除**選項。
     - 看到提示時，請重新啟動電腦。

附錄 A

何謂 Sandbox？

Sandbox 是一個術語，最能描述用來檢查檔案是否遭到未知病毒感染的技術。這個術語並非隨便挑選的，因為此方法能讓不信任的可能病毒程式碼在電腦上執行 – 但不在真正的電腦上，而是在電腦內的有限制模擬區域中。Sandbox 具備病毒預期在真正電腦中找到的所有一切。這個區域能夠很安全的讓病毒進行複製，但每一個步驟都受到嚴密的監控和記錄。病毒會將自己曝露在 Sandbox 中，由於它的動作已被記錄，因此會自動產生治療此新病毒的方法。

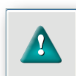
今日，新的電子郵件蠕蟲只要數秒鐘即可感染到數萬台工作站。Norman 的 Sandbox 功能已證實為可設陷捕捉新毀滅性病毒的重要工具。

附錄 B

進階系統報告器

這是專為有經驗的使用者設計的工具。它具有可讓您透過搜尋電腦上的異常情況，偵測未知間諜軟體和 rootkit 的功能。隱藏的程序、未知的自動啟動程序，以及未知的系統篩選器等可疑項目，可揭發惡意應用程式。





作業系統內部

檢視和編輯隱藏程序與驅動程式、註冊表項、安裝的篩選器及插入的 DLL 等的詳細資訊。



選擇 Internet Explorer

檢視和編輯設定、外掛程式及 cookie 的詳細資訊。



程序

檢視和編輯自動啟動程序、服務及其他程序的詳細資訊。

即使是經驗豐富的使用者，也會發現這些選項淺顯易懂，按一下「進階系統報告器」對話方塊底部的**何為 ...?** 連結將會提供有關各項主題的詳細資訊

作業系統內部

隱藏的程序

儘管目前電腦上正在執行隱藏的程序，但在使用者模式下看不到它。如果在使用者模式下隱藏了程序，這表示它已由 rootkit 隱藏。“rootkit” 通常是一個驅動程式，它隱藏惡意使用者模式程序，使標準防毒軟體看不到它。

如果您在電腦上發現隱藏的程序，很可能已有一或多個可疑項目位於此「安裝的篩選器」類別底下。這些項目就是 rootkit 本身。

註冊表項

註冊表在使用者模式與核心模式下有不同解釋。這表示某些技術可用來隱藏註冊表項不被使用者模式防毒應用程式發現。與此類技術相符的任何註冊表項都將被視為可疑。

安裝的篩選器

篩選器是一個驅動程式，或可以插入應用程式的 DLL，它們可以在接觸應用程式之前修改資料。

- **LSP (層次服務提供者)**
  LSP 是一種網路篩選器，可以在應用程式載入 WinSock 時載入到所有應用程式中，是應用程式訪問網路的常見方法。此類網路篩選器可以修改及封鎖電腦內送及外發的網路流量。此技術通常由個人防火牆和家長控制產品使用。
  惡意網路篩選器可以修改搜尋結果、監視您的網路流量、顯示不需要的廣告及將您重定向至惡意網站。
- **SSDT (系統服務分派表格)**
  這種特殊驅動程式可修改 SSDT，以篩選由所有應用程式執行的作業，例如開啟或讀取檔案，或者啟動新的應用程式。安全供應商通常會使用此技術來防止惡意應用程式對電腦進行有害變更。
  但是惡意 SSDT 驅動程式可能會取得強大的 rootkit 功能。如果您的電腦上有未知的 SSDT 驅動程式，而且您也看見一或多個隱藏的程序，則存在 rootkit 的可能性非常高。

插入的 DLL

DLL (動態鏈接庫) 是一種程式模組，會將其儲存在個別檔案中以在不同的應用程式之間共用它，或為現有應用程式提供擴展功能。關聯應用程式會於需要時載入 DLL。

- **插入的 DLL**
  可以強制應用程式載入第三方 DLL。即使應用程式的供應商沒有執行此操作的意圖，且沒有明確載入 DLL，也可以執行此操作。這是惡意軟體廣泛使用的一種技術，因為 DLL 中的程式碼模組可以完全控制應用程式。且它可以代表應用程式執行作業，欺騙作業系統與安全軟體，使它們相信是應用程式執行了作業。
  將 DLL 插入其他應用程式有幾個合法用途。例如在應用程式崩潰時執行調試。但一般而言，將 DLL 插入其他應用程式的應用程式是設計不當的軟體，或是惡意軟體。
  如果您發現系統中有插入的 DLL，您應該特別小心。您應該移除不是來自完全信任的供應商的任何 DLL。實際上，您從 Internet 下載及安裝的軟體甚至也可能是特洛伊木馬。

隱藏的驅動程式

儘管目前電腦上正在執行隱藏的驅動程式，但在使用者模式下看不到它。在使用者模式下隱藏的驅動程式具有 rootkit 功能。驅動程式會在硬碟上隱藏其檔案、其註冊表項，其記憶體空間。

Internet Explorer

設定

檢視及編輯 Microsoft Internet Explorer 的設定。

外掛程式

瀏覽器的外掛程式可為您提供其他功能，例如工具列與搜尋增強功能，但它也可能會提供不需要的廣告，甚至還會窺探您的上網習慣與密碼。

- **瀏覽器幫助對象**
  - 「瀏覽器幫助對象」(BHO) 是 Internet Explorer 的外掛程式，旨在修改瀏覽器的內送流量或外發流量。它是間諜軟體應用程式最常用的一種外掛程式，因為它可以輕鬆擷取傳送至瀏覽器與來自瀏覽器的所有資料。
- **工具列**
  - 工具列是 Internet Explorer 的外掛程式，會在瀏覽器的工具列窗格中建立新項目。廣告軟體應用程式可以使用這種類型的外掛程式來顯示廣告。
- **URL Search Hook**
  - Search Hook 旨在重定向輸入的網址，且它可以協助解析不正確或不完整的位址。例如，預設會將 norman.com 轉換為 http://www.norman.com。廣告軟體應用程式可以使用這種類型的外掛程式來將您重定向至其他網站。
- **其他**
  - 其他外掛程式可以將功能表選項或使用者面板新增至瀏覽器。廣告軟體應用程式可以使用這種類型的外掛程式來顯示廣告。



注釋：儘管特定外掛程式不是旨在修改流量及窺探使用者資料，但所有外掛程式在技術上都能夠執行這些操作。

Cookie

Cookie 是在您造訪了某網頁後置於暫存 Internet 檔案中的小檔案。

- **誤解**
  - 對於 cookie 有一些常見的誤解，認為它們是惡意的、它們會產生彈出訊息與不需要的廣告，以及它們會危害您的電腦。確實有一些防間諜軟體供應商將它們列為間諜軟體，甚至還對某些 cookie 發出警報，特別是在所謂「跟蹤 cookie」的情況下。
  - Cookie 沒有危險，而且不會危害您的電腦。因此，您在此對話方塊中顯示的 cookie 沒有威脅。但是如果您願意，可以選擇移除它們。
- **使用 cookie**
  - Web 伺服器使用 cookie 來區分使用者，以及保留狀態。如果刪除 cookie，將會失去使用者偏好設定、購物圖表，以及記住您的登入憑證的系統 (即使在多次造訪之後)。舉例來說，系統將會要求您再次登入。
- **跟蹤 cookie**
  - 某些網站使用第三方 cookie 來跟踪您在網站之間的移動。有人認為這侵犯了他們的隱私權。但您造訪的 Web 伺服器也可以在伺服器之間直接執行此類跨網站通訊，而無須依賴跟踪 cookie。
  - 此工具不會區分跟踪 cookie 與正常 cookie，因為它們之間唯一的差異是跟蹤 cookie 由第三方維護。從惡意軟體的觀點來看，兩者的危險程度相同。

程序

自動啟動

如果您的電腦上安裝了合法或惡意應用程式，該程式通常會想要在每次啟動您的電腦時自動啟動。想要自動啟動的程式可以指示作業系統使用與目前使用者相同的權限自動啟動其本身，或者也可安裝以升級權限執行的背景服務。此入侵防範應用程式可將這兩類嘗試都停止。



注釋：自動啟動功能並不包含 CD 或 USB 隨身碟的自動執行功能。

服務

服務是一個背景程序，它會於每次電腦啟動時啟動。這是正常行為。

Norman 辦公室

丹麥
Norman Data Defense Systems AS
Blangstedgårdsvej 1,
DK-5220 Odense SØ
電話：　+45 63 11 05 08
傳真：　+45 65 90 51 02
電子郵件：info@normandk.com
網址：　www.norman.com/dk

德國
Norman Data Defense Systems GmbH
Zentrale, Gladbecker Str. 3,
D-40472 Düsseldorf
電話：　+49 0211 5 86 99-0
傳真：　+49 0211 5 86 99-150
電子郵件：info@norman.de
網址：　www.norman.com/de

西班牙
Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1,
28224 Pozuelo de Alarcón MADRID
電話：　+34 91 790 11 31
傳真：　+34 91 790 11 12
電子郵件：norman@normandata.es
網址：　www.norman.com/es

法國
Norman France
8 Rue de Berri,
F-75008 Paris
電話：　+33 1 42 99 94 14
傳真：　+33 1 42 99 95 01
電子郵件：info@norman.fr
網址：　www.norman.com/fr

義大利
Norman Data Defense Systems
Centro Cassina Plaza,
Via Roma, 108
20060 Cassina de'Pecchi (MI)
電話：　+39 02 951 58 952
傳真：　+39 02 951 38 270
電子郵件：info@normanit.com
網址：　www.norman.com/it

荷蘭
Norman SHARK B.V.
Postbus 159,
2130 AD Hoofddorp
電話：　+31 23 789 02 22
傳真：　+31 23 561 31 65
電子郵件：support@norman.nl
網址：　www.norman.com/nl

挪威
Norman ASA
Headquarter and sales Norway
Hovedkontor og salg Norge
敬請光臨：Strandveien 37, Lysaker
郵寄：PO Box 43, N-1324 Lysaker
電話：　+47 67 10 97 00
傳真：　+47 67 58 99 40
電子郵件：norman@norman.no
網址：　www.norman.com/no

瑞士
Norman Data Defense Systems AG
Münchensteinerstrasse 43
CH-4052 Basel
電話：　+41 61 317 25 25
傳真：　+41 61 317 25 26
電子郵件：norman@norman.ch
網址：　www.norman.com/ch

瑞典
Norman Data Defense Systems AB
Södra Grytsgatan 7, 2tr,
Norrköping Science Park
S-602 33 Norrköping
電話：　+46 11 230 330
傳真：　+46 11 230 349
電子郵件：sales.se@norman.com
網址：　www.norman.com/se

英國
Norman Data Defense Systems (UK) Ltd
Exchange House,
494 Midsummer Boulevard
Central Milton Keynes,
MK9 2EA
電話 1：　+44 08 707 448 044
電話 2：　+44 01 908 255 990
傳真：　+44 08 701 202 901
電子郵件：info@normanuk.com
網址：　www.norman.com/en-uk

美國
Norman Data Defense Systems Inc.
9302 Lee Highway,
Suite 950A,
Fairfax, Virginia 22031
電話：　+1 703 267 6109
傳真：　+1 703 934 6368
電子郵件：norman@norman.com
網址：　www.norman.com/en-us



Norman ASA 是全球資料安全、網際網路防護及分析工具領域的領導廠商。與其他競爭對手不同，Norman 透過其 Sandbox 技術提供獨特、主動式的防護。專注於其主動式防毒技術的同時，Norman 還組建聯盟，以便提供全範圍的資料安全服務。

Norman 成立於 1984 年，總部位於挪威，歐洲大陸、英國與美國為其主要市場。

NORMAN®